Programma van Eisen OSO’17
Versie: 1.1/20170316

Inhoudsopgave

Inleiding 11
OSO specificatie 12
Externe informatiebronnen 12
Communicatie 12
Algemene Eisen 13
Algemene eisen en randvoorwaarden 13
Inzage Dossiers 13
Bewaartermijn Dossiers 13
Bewaartermijn Dossier verzoeken tbv Notficatie 13
Bewaartermijn KoppelSleutel 13
Overige technische randvoorwaarden 14
Foutmeldingen 14
Adressering 14
Logging 15
Timing 15
Omvang berichten 16
'Zippen' van bijlagen 16
Specifieke Eisen 17
Functionele eisen per type systeem 17
Functionaliteit voor alle typen systemen 17
Functionaliteit voor Bronsystemen (exclusief ondersteuning SWV PaO) 18
Use cases voor Doelsystemen (exclusief ondersteuning SWV PaO) 19
Aanvullende Use Cases voor LASsen PaO uitwisseling 19
Aanvullende Use Cases voor SWV's en RP's PaO uitwisseling 20
Inhoudelijke Eisen 21
Toepassen EduStandaard OSO Gegevensset 21
Dossier-formaat en -controle 21
Eis aan Bronsysteem 21
Eis aan Doelsysteem 21
Selectief uitleveren 21
Telefoonnummer validatie 22
Wijzigingen in OSO’17 23
Hoofdwijzigingen 23
Aanvullende wijzigingen 23
Wijzigingsvoorstellen (orginele documenten) 23
Architectuur 24

Architectuur 24
PaO Proces 24
Context 24
Voorzieningen in OSO infrastructuur 25
Registratie SWV aanleverpunten 25
Afspraak gegevensset 26
OSO gegevensset 26
Versies en nummering 27
Gegevensset 27
Bundels 27
Validatieversie 27
Beveiliging 28
Beveiligingsrequirements 28
Kwalificatie Leveranciers 28
Aangesloten leveranciers 28
Certificaten 29
Register 29
Controles binnen het proces 30
Logs en monitoring 31
Uitgangspunten 32
Doel 32
Basisprincipes 32
Proces 33
Dossier uitwisseling 33
Dossier uitwisseling 33
Aanleverpunten 35
Notificatie na Aanvraag (Schooluitwisseling) 36
Notificatie met KoppelSleutel (Passend Onderwijs) 36
Push en Pull 36
Sleutel tussen Systemen 37
Uitwisselen PaO berichten 38
Versturen Dossier tbv Aanvraag 38
Versturen Terugkoppeling over Aanvraag 39
Registreren Aanleverpunt 41
Context 41
Basisscenario 41
Overzicht meldingen 42

Ping Traffic Center 43
Context 43
Basisscenario 43
Sequence Diagram Ping Service 44
Overzicht meldingen 45
Controleren Aanleverpunt 46
Context 46
Basisscenario 47
Request 47
Response 48
Overzicht meldingen 48
Opvragen Aanleverpunten 49
Basisvariant: Opvragen AP informatie 49
Preconditie 49
Postconditie 49
Request 50
Response 51
Uitzonderingen en meldingen 51
Samenstellen Dossier 52
Context 52
Onderliggende use cases 52
Wettelijke eisen 52
Dataminimalisatie 52
Inzage en toestemming 53
Aanvullende eisen 53
Validatie tegen OSO standaard voorafgaand aan verzenden 53
Registreren Verzameldatum 53
Uitvoeren Inzage 54
Registreren Inzage 57
Context 57
Normal flow 57
Alternatives 57
Samenstellen Inhoud Dossier 58
Profielen en Blokken 58
Functionele eisen 58
Valideren Dossier 59
Klaarzetten Dossier 60

Gereed zetten dossier 60
Basisscenario 60
Initiëren notificatie 61
Basisvariant: Notificatie voor Dossier overdracht 61
Basisvariant: Notificatie voor aanvraag bij Samenwerkingsverband 61
Basis scenario 61
Uitzonderingen en meldingen 63
Verwerken openstaande verzoeken 67
Context 67
Randvoorwaarden en eisen 67
overstap 68
Preconditie 68
Postconditie 68
Aanroep en antwoord 68
Tonen aanvragen 70
Tonen ontvangen dossier aanvragen 70
aanvraag 71
Preconditie 71
Postconditie 71
Aanroep en antwoord 71
Notificeren van Doelsystemen 73
Context 73
Juridische randvoorwaarden 73
Overige randvoorwaarden 73
Context 74
Onderliggende use cases 74
Notificatie mechanisme 74
Tonen Aanvragen 76
Notificatie dossier aanvragen 76
Versturen Notificatie 77
Basisvariant: Notificatie na ontvangst DocumentRequest 77
Basisvariant: Notificatie voor aanvraag bij SWV 77
Basisscenario 77
Uitzonderingen en meldingen 78
Tonen Notificaties 79
Tonen ontvangen Notificaties 79
Initiëren Terugkoppeling 79

Preconditie 79
Postconditie 79
Basis scenario 80
Uitzonderingen en meldingen 80
Aanroep en antwoord 83
Versturen Terugkoppeling 84
Preconditie 84
Postconditie 84
Basis scenario 85
Uitzonderingen en meldingen 85
Aanroep en antwoord 86
Uitvoeren opvraag sessie 87
Context 87
Preconditie 87
Postconditie 87
Basis Scenario 87
Aflopen Aanleverpunten 88
Doorlopen sessie 89
Context 89
Preconditie 89
Postconditie 89
Basis Scenario 89
Aflopen Aanleverpunten 90
Initiëren sessie 91
Basisvariant: Overstapdossier 91
Variant: Specifieke Aanleverpunt bevragen 91
Basisvariant: Aanvraag bij Samenwerkingsverbanden 91
Basis scenario 92
Uitzonderingen en meldingen 92
overstap 96
Overstap variant 96
Preconditie 96
Postconditie 96
Aanroep en antwoord 96
Variant: Specifieke Aanleverpunt bevragen 100
Aanroep en antwoord 100
Opvragen dossier 102

Basisvariant: Overdracht van Dossier 102
Basisvariant: Aanvraag bij Samenwerkingsverbanden 102
Basisscenario 102
Variant: Opvragen met AanvraagDatum 104
Uitzonderingen en meldingen vanuit de Sessie controle 104
Uitzonderingen en meldingen 105
Controleren Sessie 109
Preconditie 109
Postconditie 109
Basisvariant 109
Uitzonderingen en meldingen 110
Aanroep en antwoord 111
aanvraag 113
Uitwisseling tbv aanvraag bij Samenwerkingsverband (SWV) variant 113
Preconditie 113
Postconditie 113
Aanroep en antwoord 113
Opvragen met Koppelsleutel ipv Zoeksleutel 115
Importeren Dossier 116
Tonen inhoud binnengekomen Dossier 116
Uitwisseling voor aanvragen bij Samenwerkingsverband Passend Onderwijs 116
Meervoudige ontvangst 117
Afmelden Sessie 118
Context 118
Preconditie 118
Postconditie 118
Basic Scenario 118
Uitzonderingen en meldingen 119
Aanroep en antwoord 123
beveiliging 125
uitgangspunten 126
Uitgangspunten voor de beveiliging van OSO 126
scope 126
Scope van de beveiligingsmaatregelen 126
Traffic Center 126
Aangesloten Systemen 126
Eindgebruiker 127

opzet paginas 127
versleuteling bsn 128
Versleuteling persoonsgebonden nummer (de zoeksleutel) 128
certificaten webservice 131
Leveranciers van certificaten 131
Geldigheidsduur (maximale termijn) 131
Eisen 131
Verklaring 131
Type certificaat 131
Eisen 131
Verklaring 131
Sterkte en type sleutel 132
Eisen 132
Verklaring 132
Wisselen sleutel 133
Eisen 133
Verklaring 133
Ondertekeningsalgoritme 133
Eisen 133
Verklaring 133
Type CSP validatie (DV, OV, EV) 134
Eisen 134
Verklaring 134
Certificaat keten 134
Eisen 134
Verklaring 135
client certificaten 136
Leverancier van certificaten 136
Eisen 136
Verklaring 136
Aanvullende informatie betreffende CSPs 137
Verklaring ten aanzien van DUO ODOC certificaten 137
Geldigheidsduur 137
Sterkte sleutel 137
Wisselen sleutel 137
Ondertekeningsalgoritme 137
Certificaat keten 138

Gebruik van het certificaat 138
Aanmelden van het certificaat 138
Implementatie Client Certificate Authentication 138
certificaat validatie 138
Rijkwijdte 138
Verloopdatum 139
Eisen 139
Verklaring 139
Intrekkingsstatus 139
Eisen 139
Verklaring 139
Validatie certificaat keten 139
Eisen 139
Verklaring 139
Certificaat voor de webservice geldig op het aangegeven domein? 140
Eisen 140
Verklaring 140
Client certificaat geldig binnen de OSO keten? 140
Eisen 140
Verklaring 140
client authentication windows 140
Register 141
Issuer certificaten importeren 141
IIS configuratie 142
Testen 142
Proxy 143
Issues 143
protocollen 144
HTTPS 144
HSTS 144
TLS 145
Versie 145
Ciphersuites en PFS 146
Cipher volgorde 149
Renegotiation 149
Compression 150
Sessie hervatting 150

ServerNameIndication 150
Certificate Authorities (issuers) 152
Fallback SCSV (protocol downgrade attack prevention) 153
Public key pinning 153
informatiebeveiliging per interactie 154
Informatiebeveiliging per interactie 154
controle procedure 156
Controle procedure naleving beveiligingseisen 156
Technische test 156
Procedure bij (vermoeden van) misbruik 158
Procedure bij (vermoeden van) misbruik 158
geldigheid 158
Geldigheid van de beveiligingseisen 158
FAQ 159
Het is onduidelijk hoe de 'SAAS certificaten' werken als één (1) leverancier meerdere SaaS applicaties aanbiedt 159
Welke stappen moet ik als 'OSO 15 leverancier' doen om met 'SAAS certificaten' te gaan werken? 159
Blijven de huidige Aanleverpunten geldig/actief? 160
Hoe moet op Windows(IIS) servers TLS geconfigureerd worden 160
Implementatie 'work around' TLS op .NET niet (altijd) mogelijk 160
OSO:Releases 161
Index 162
Index 162
Woordenlijst 164

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 schoolsystemen 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.

Deze website fungeert als "Programma van Eisen" en als "ontwerpspecificatie" voor partijen die willen aansluiten op OSO. De informatie op deze site is daardoor voornamelijk technisch van aard. Voor scholen en eindgebruikers is actuele en relevante informatie beschikbaar op de volgende website: Overstapservice Onderwijs. Daarnaast zijn nog twee websites van belang:

- 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 leveranciers van schoolsystemen samen om de overdracht van leerlinginformatie tussen scholen in het PO en VO te faciliteren en optimaliseren.

- Op deze pagina is een overzicht van aangesloten scholen te vinden: [1]
- Op deze [pagina] is een overzicht van aangesloten systemen te vinden.

Voor inhoudelijke vragen kunt u contact opnemen met OSO support.

OSO specificatie

Wijzigingen in OSO'17

Algemene eisen
Inhoudelijke eisen
Functionele eisen
Beveiligingseisen

Architectuur

Index OSO'17

Externe informatiebronnen

- EduStandaard OSO (dossier standaard)
- Kennisnet Validatie Service
- Woordenlijst

Communicatie

Overstap Service Onderwijs site

Atom Feed wijzigingen OSO wiki

Algemene Eisen

Algemene eisen en randvoorwaarden

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 ondersteunen. OSO faciliteert alleen het beveiligd transport van deze gegevens.

Inzage Dossiers

Voorafgaand aan verzending dient (voor een aantal typen overstap) het Dossier in te worden gezien door de ouders/verzorgenden. De eisen en randvoorwaarden die hiervoor gelden worden hier beschreven.

Bewaartermijn Dossiers

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, is advies om het overstapdossier (het complete xml bericht inclusief bijlagen) nog twee jaar te bewaren. Daarna dient het dossier te worden vernietigd.

Bewaartermijn Dossier verzoeken tbv Notficatie

In OSO'17 is deze termijn ingesteld op 6 (kalender)maanden of tot het einde van het OSO'17 'seizoen' (juni/juli 2017). De verzoeken tot levering hoeven niet overgenomen te worden in OSO'18.

Bewaartermijn KoppelSleutel

De bewaartermijn van KoppelSleutels is nog aan juridisch onderzoek onderhevig. Vooralsnog geldt dat een KoppelSleutel een heel OSO seizoen (van moment aanmaken tot aan uitrol volgende OSO versie ('Big Bang') geldig is en toegepast mag worden.

Overige technische randvoorwaarden

Foutmeldingen

In OSO'17 worden standaard foutmeldingen voor Eindgebruikers geïntroduceerd. Als een fout of uitzondering optreedt dan **moet** een systeem zowel:

- de code uit de 'Resultaat' kolom
- én de foutmelding uit de kolom 'Melding aan Eindgebruiker'

in de tabellen bij de Use Case beschrijvingen tonen aan de Eindgebruiker.
De lijst met standaard foutmeldingen geldt als 'referentie implementatie'. In plaats van de standaard foutmelding mag een Leverancier kiezen eigen foutmeldingen toe te passen (ook in dat geval **moet** de code's uit de Resultaat kolom getoond worden.)

De complete en bijgewerkte lijst met foutmeldingen is hier te vinden. Deze lijst is de toe te passen lijst(!). De meldingen zijn ook toegevoegd in de use case beschrijvingen onder de kop 'Uitzonderingen en meldingen', maar de **meldingen in de (xls-)lijst zijn leidend(!)**.

Adressering

In de adressering van OSO berichten worden altijd vier velden toegepast:

- bronBRIN
- bronAPindex
- doelBRIN
- doelAPindex

Hierbij worden twee uitgangspunten toegepast:

1. Doel en Bron worden hier absoluut gebruikt, volgens de rol die het desbetreffende systeem uitvoert in de transactie
2. De velden worden ingevuld wanneer dit mogelijk is (en zijn anders leeg). (Bijvoorbeeld: In het geval van een overdrachtRequest kunnen alleen de doelBRIn, doelAPindex en bronBRIN ingevuld zijn, omdat het doelsysteem dat dit request verstuurd nog geen idee heeft welke aanleverpunten afgelopen moeten worden).

Logging

Een op OSO aangesloten systeem moet gegevens over verzonden en ontvangen berichten en opgetreden fouten opslaan en beschikbaar kunnen maken voor twee doelen:

- het kunnen achterhalen welk dossier wanneer tussen welke systemen is uitgewisseld en welk gebruikersaccount daar opdracht toe gaf (juridische eis)
- 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 (operationele toepassing)

Richtlijnen Logging

Om aan beide eisen te kunnen voldoen gelden de volgende richtlijnen voor de logging binnen doel- en bron- systemen:

- **De BRIN, uit het PKI certificaat van het systeem waarmee gecommuniceerd wordt, wordt gelogd**
- De SessieID en **gebruikersaccount** (binnen het systeem) worden gelogd
- 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.
- Log regels bevatten altijd het geldige sessie-id (wanneer dit is toegekend).
- In de logregels moet of de ZoekSleutel of de Koppelsleutel (indien van toepassing) worden vastgelegd.
- 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.
- 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 na het moment van overdracht van het dossier.

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.

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 slaan. Anderzijds is het loslaten van een bovengrens aan de dossiergrootte onverstandig uit praktische overwegingen. De volgende bestandsgrootte's zijn daarom afgesproken:

- Bijlage: maximaal 10MB
- Compleet dossier: maximaal 30MB.

'Zippen' van bijlagen

Documenten die als bijlage aan een dossier worden toegevoegd, worden als een in Base64 gecodeerd zip bestand opgenomen in het dossier. In OSO wordt hiervoor de **MIME Base64 content-transfer-encoding standaard**, zoals beschreven in RFC 2045, toegepast. Deze variant maakt gebruik van dezelfde tekenset als ?Standaard? Base64 (zoals beschreven in RFC 4648, hoofdstuk 4 variant 1), maar kapt regels af op 76 tekens of minder, gescheiden door een CRLF(?\r\n?). Daarnaast worden bij het decoderen alle ?vreemde? tekens genegeerd. NB: Deze codering wijkt af van die toegepast voor de zoeksleutel(!).

Specifieke Eisen

Functionele eisen per type systeem

In OSO'17 wordt de functionaliteit uitgebreid met:

- Selectief uitleveren.
- Koppelen van Samenwerkingsverbanden Passend Onderwijs.

Er geldt dat in OSO'17 alle bronsystemen Selectief Uitleveren moeten ondersteunen. Voor de ondersteuning van aanvragen bij Samenwerkingsverbanden geldt dat dit verplicht is voor systemen in het VO en optioneel voor PO systemen.

Functionaliteit voor alle typen systemen

Beschrijving	Use case	Verplicht	Opmerkingen
Aanroep voor het testen van de beschikbaarheid van het Traffic Center	Pingen van Traffic Center	Verplicht	
	Registreren van een Aanleverpunt	Verplicht	Bij het registreren van een Aanleverpunt kan met het controleren van de APsleutel de invoer van de eindgebruiker gevalideerd worden.
Registreren vanuit een Systeem van een Aanleverpunt bij het TC	Controleren van de AanleverpuntSleutel	Optioneel	Valideren van de invoerde waarden in een Systeem bij een Aanleverpunt op basis van de Aanleverpuntsleutel.
	Opvragen van Aanleverpunten	Optioneel	Door te filteren op APsleutel kan met deze aanroep informatie over bewerkt Aanleverpunt worden opgehaald.
Aanroep voor het opvragen van informatie over AanleverPunten bij het Traffic Center	Opvragen van Aanleverpunten	Optioneel	

Functionaliteit voor Bronsystemen (exclusief ondersteuning SWV PaO)

Beschrijving	(Deel)processtap	Use case	Opmerkingen
Samenstellen en klaarzetten Dossier	Laten inzien Dossier	Registreren van inzage Dossier	Vindt plaats 'binnen' systeem, geen directe interactie met OSO
		Selectief samenstellen Dossier	
	Samenstellen van het Dossier	Dossier controleren tegen OSO standaard	Voorafgaand aan versturen controleert Bronsysteem Dossier tegen Edustandaard Gegevensset OSO
		Dossier klaarzetten voor Scholen	Voordat Doelsysteem Dossier kan opvragen moet in Bronsysteem aangegeven worden dat Dossier gereed is en beschikbaar voor specifieke scho(o)l(en)
Verwerken Verzoeken en Notificaties	Verwerken openstaande verzoeken	Tonen ontvangen verzoeken	Vindt plaats 'binnen' systeem, geen directe interactie met OSO
	Versturen Notificatie	Versturen NotificatieMelding naar TC	Na klaarzetten Dossier voorafgaand aan verzenden van Notificatie
		Versturen Notificatie naar Doelsysteem	Melden aan Doelsysteem dat Dossier beschikbaar is gekomen
Afhandelen verzoek levering Dossier		Controleren van een Sessie	Na ontvangst van verzoek tot levering van Dossier
		Doorlopen Dossier verzoek	Als antwoordende partij bij Opvragen Dossier

Use cases voor Doelsystemen (exclusief ondersteuning SWV PaO)

Algemeen	(Deel)processtap	Use case	Opmerkingen
Verwerken Verzoeken en Notificaties	Ontvangen Notificatie naar Doelsysteem	Tonen ontvangen Notficaties	Reageren op binnenkomende Notificaties
	Doorlopen opvraag Sessie	Initiëren van een Sessie	Geïnitieerd door eindgebruiker of ontvangst van Notificatie
		Opvragen van een Dossier	Initiator/vragende partij bij Opvragen Dossier
Uitvoeren opvraag Sessie	*Doorlopen opvraag Sessie*	*Controleren van een Sessie*	*Functionaliteit voor Bronsysteem(!)*
	Doorlopen opvraag Sessie	Importeren en tonen van een Dossier	Na een geslaagde overdracht
		Afmelden van een Sessie	Na het ontvangen van een Dossier of het aflopen van alle Aanleverpunten

Aanvullende Use Cases voor LASsen PaO uitwisseling

Algemeen	(Deel)processtap	Use case	Opmerkingen
Uitwisseling voor Aanvraag bij SWV PaO	|Initiëren Aanvraag vanuit LAS	Aanleverpunt selecteren voor Notificatie	Adressering naar SWV
		Versturen NotificatieMelding naar TC	Aanvragen KoppelSleutel bij TC
		Versturen Notificatie naar Doelsysteem	Versturen KoppelSleutel naar SWV systeem
	Opvragen Dossier met KoppelSleutel	*Opvragen van een Dossier*	*Functionaliteit voor SWV systeem(!)*
Terugkoppeling vanuit SWV naar School	*Initiëren terugkoppeling*	*Versturen TerugkoppelingMelding naar TC*	*Functionaliteit voor SWV systeem(!)*
	Ontvangen Terugkoppeling	Versturen Terugkoppeling naar Bronsysteem	Als ontvangende partij

Aanvullende Use Cases voor SWV's en RP's PaO uitwisseling

Algemeen	(Deel)processtap	Use case	Opmerkingen
Uitwisseling voor Aanvraag bij SWV PaO	Initiëren Aanvraag vanuit LAS	Versturen Notificatie naar Doelsysteem	Afhandelen ontvangst Notificatie met KoppelSleutel
	Opvragen Dossier met KoppelSleutel	Opvragen van een Dossier	Opvragen Dossier met KoppelSleutel. Automatisch gestart na ontvangst Notificatie(!)
Terugkoppeling vanuit SWV naar School	Initiëren terugkoppeling	Versturen TerugkoppelingMelding naar TC	Opvragen url AP bij TC
	Ontvangen Terugkoppeling	Versturen Terugkoppeling naar Bronsysteem	Als initiérende/verzenden partij

Inhoudelijke Eisen

Toepassen EduStandaard OSO Gegevensset

Dossiers verstuurd via de OSO infrastructuur moeten altijd voldoen aan de EduStandaard OSO gegevensset.

Dossier-formaat en -controle

Binnen OSO wordt gewerkt met één gestandaardiseerd formaat voor het Dossier; in OSO'17 wordt de Standaardversie: **2017.1.1** gebruikt.

Eis aan Bronsysteem

Een Bronsysteem moet voorafgaand aan verzending controleren dat het Dossier hieraan voldoet.

Eis aan Doelsysteem

- Een ontvangend systeem mag voorafgaand aan het importeren een Dossier valideren tegen de correcte versie van de Standaard. Dit is niet verplicht.
- Bij de verdere verwerking en import van het Dossier moet een ontvangend systeem dusdandig robuust zijn dat subversies van het Dossier verwerkt kunnen worden. Met subversies worden alle versies achter onder de hoofdversie bedoelt, dus bij een hoofdversie 2017.1 moeten zowel Dossiers van versie 2017.1.0 én 2017.1.1 worden geaccepteerd.)

Selectief uitleveren

Om bronscholen in staat te stellen de inhoud van een dossier aan te passen, zodanig dat de inhoud recht doet aan het doel van de overdracht (doelbinding) en daarbij rekening te houden met zowel de administratieve last voor de school als de impact hiervan voor systeembouwers. Er is gekozen om te gaan werken met profielen in combinatie met blokken van velden. Per profiel wordt aangegeven welke blokken verplicht, verboden dan wel optioneel zijn. De indeling per profiel is terug te vinden in de beschrijving van de OSO gegevensset.

Een school kan optionele blokken van velden uit het dossier verwijderen, zodat deze niet meegestuurd worden. De ontvangende school kan in het dossier zien of blokken bewust uitgezet zijn. Dit wordt door de pdf-viewer (door Kennisnet geleverd) ondersteund; ontvangende systemen zijn niet verplicht dit binnen hun systeem te tonen

In de gegevensset wordt in OSO?17 gewerkt met profielen. Een profiel verdeelt de gegevensset in blokken van velden. Per type uitwisseling (POVO, POPO, etc.) wordt aangegeven of een blok verplicht of optioneel is.

Zie ook: Selectief samenstellen Dossier.

Telefoonnummer validatie

Bij het invoeren of wijzigen van een telefoonnummer in een ?telefoon veld? (communicatiesoort == ?telefoon?) in OSO, dient een systeem:

1. Het nummer gecontroleerd mbv de Google library ?libphonenumber?
2. Alleen nummers die door deze library als ?valid? worden beschouwd mogen geaccepteerd
3. Het nummer wordt vervolgens in het ?**E164? formaat** opgeslagen (output van library)

Bij het opslaan van het telefoonnummer wordt bij voorkeur/aanbevolen om de volgende structuur toe te passen: <telefoonnummer (E164 formaat)><spatie><aanvullende informatie>.

Op die manier kan er wel aanvullende informatie worden toegevoegd bij een telefoonnummer en wordt het interpreteren en controleren van telefoonnummers eenduidiger.

NB: Als eindgebruikers het telefoonnummer niet verbeteren of op enige wijze het telefoonnummer niet gecorrigeerd raakt, dan is het toepassen van 'onmogelijke telefoonnummers' geen reden om een dossier niet te verzenden of te weigeren bij importeren. Door gebruikers te attenderen en begeleiden bij het invoeren van bruikbare telefoonnummers zal (hopelijk) de kwaliteit van deze gegevens binnen OSO verbeteren.

Wijzigingen in OSO’17

Hieronder volgen de wijzigingsvoorstellen voor OSO'17 zoals die in Regiegroep en Technisch Overleg besproken zijn:

Hoofdwijzigingen

- Selectieve uitlevering (inclusief nieuwe Dossier standaard)
    - Bronsystemen: Aanbieden user interface voor het kunnen uitschakelen ('opt out') van 'blokken' door eindgebruiker
    - KVS/Bronsystemen: Controle op correcte toepassing hiervan
    - PDF-viewer/Doelsystemen: Tonen in/uit-geschakelde 'blokken'
- Uitbreiden OSO keten met Samenwerkingsverbanden Passend Onderwijs
    - Verplicht voor VO systemen, optioneel voor PO systemen
    - Uitbreiding Notificatie met KoppelSleutel
    - Uitbreiding met Terugkoppeling bronsystemen (LAS)

*** NB: Ook aanpassing voor systemen die dit niet aanpassen (operatie niet ondersteund melding)*

- ~~Toevoegen PKI ODOC (DUO) certificaten als SAAS certificaat~~ (Wijzigingsvoorstel afgewezen)
- Standaardfoutmeldingen naar eindgebruikers
- Langere periode voor geldigheid verzoek tot levering voor Notificaties
- Opvragen Aanleverpunt informatie bij TC

Aanvullende wijzigingen

1. [Standaard telefoon controle en formaat]
2. Controle op versie van dossier naar twee digits
3. Controleren Aanleverpunt uitgebreid met optionele parameter 'Doel'

Wijzigingsvoorstellen (orginele documenten)

1. Selectief uitleveren van Dossiers vanuit Bronsystemen invoeren binnen OSO.
2. Aansluiten Samenwerkingsverbanden Passend Onderwijs op OSO
    1. Nadere uitwerking van dit voorstel (Samenvatting van besluiten/ontwerpbeslissingen bijeenkomst Experts op 20170213. Betreft met name uitwisseling naar Samenwerkingsverbanden Passend Onderwijs en de Terugkoppeling.)
3. ~~Toepassen PKI ODOC (DUO) naast PKI OVerheid als SAAS certificaat~~
4. Standaard foutmeldingen voor eindgebruikers toepassen in aangesloten systemen
5. Opvragen informatie over Aanleverpunten bij TC mogelijk maken.

Architectuur

Architectuur

- Uitgangspunten
- Uitwisselproces
- Uitwisseling Passend Onderwijs
- Edustandaard Afpraak OSO gegevensset
- Beveiliging
    - Beveiligingsmaatregelen
- Systeemlandschap

PaO Proces

Context

Scholen zijn aangesloten op SWV?s om de regelingen rond de wet Passend Onderwijs uit te voeren. Hiervoor wordt informatie vanuit schoolsystemen naar systemen van de SWV?s. Deze systemen zijn opgebouwd als een regionaal platform (RP): ze hebben allemaal naast een deel voor het SWV ook een deel voor scholen. In het schooldeel worden aanvragen voorbereid door medewerkers van een school, waarna de aanvraag binnen het RP wordt doorgestuurd naar het SWV deel. In het SWV gedeelte van het RP wordt de aanvraag verder verwerkt door medewerkers van het SWV. Doordat het aantal soorten regelingen en arrangementen dat wordt aangevraagd bij SWV?s aanzienlijk is en deze regelingen in regio?s op verschillende manieren worden uitgevoerd, bieden de RP?s scholen en SWV?s op maat ingerichte formulieren en werkwijzen. Voor scholen (en indirect SWV?s) is er een grote winst te behalen als de informatie die in schoolsystemen aanwezig is, verzonden kan worden naar de RP?s bij het doen van een aanvraag. Een school start een aanvraag voor een regeling (meestal TLV, maar ook andere) door gegevens vanuit haar LAS te sturen naar het schooldeel van het RP met behulp van OSO. Dit is een eenmalige overdracht van gegevens, waarbij de benodigde gegevens heel dicht liggen bij die van de OSO gegevensset. Deze overdracht bevat niet de gegevens over de aanvraag, die worden in het schooldeel van het RP toegevoegd.
De uitwisseling van scholen met SWV?s wijkt af van ?normale OSO uitwisselingen? op vijf belangrijke punten:

- De uitwisseling wordt alleen gestart bij doen van een aanvraag door een school bij een SWV
- Het initiatief van de uitwisseling ligt bij de bronschool
- Het PGN van de leerling mag niet als zoeksleutel worden gebruikt
- Het PGN van de leerling mag niet worden verstuurd in het dossier
- Naar aanleiding van een uitwisseling kan een SWV een bericht terugsturen (Terugkoppeling)

Voorzieningen in OSO infrastructuur

Voor het aansluiten van de SWV?s op OSO zijn drie uitbreidingen aan de OSO infrastructuur ingevoerd in OSO'17:

- Uitbreiden notificatie met notificatie-met-koppelsleutel
- Uitbreiden uitwisseling met uitwisseling-via-koppelsleutel
- Nieuw aanleverpunt type ?samenwerkingsverband?

Ook wijkt het formaat van het dossier af van het ?normale? overstapdossier. Hiervoor is een (aantal) extra profiel(en) nodig in de gegevensstandaard OSO. (Omdat de uitwisseling van gegevens plaats vindt met als doel het doorleveren naar het SWV, is er geen sprake van een ?binnenBRIN? overdracht (ondanks dat de gegevens binnen de school blijven.) Deze profielen worden beschreven in het voorstel voor de nieuwe gegevensset 2017.1. De invulling van de profielen voor deze uitwisseling zal niet in dit stuk worden besproken.

Registratie SWV aanleverpunten

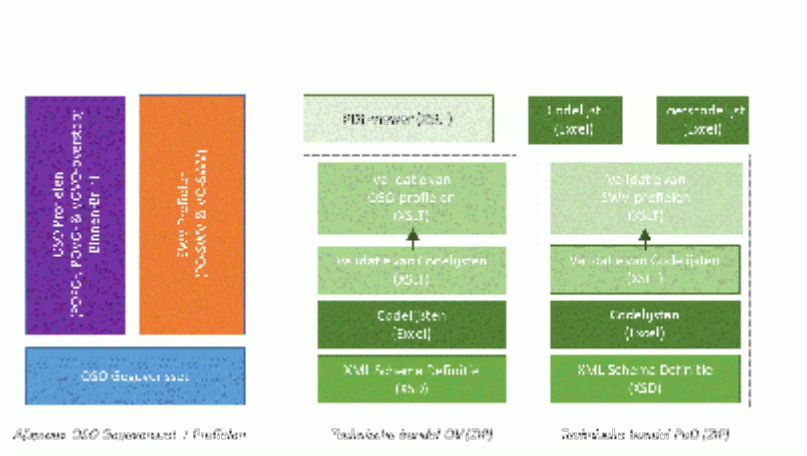
Alle bekende systemen voor SWV?s kennen de opzet van regionale platforms (RP). Voor het doen van een aanvraag bij een SWV stuurt de school daarbij eerst het dossier naar het eigen (school)deel van het RP. Daarvoor moet de schoolmedewerker weten welk aanleverpunt gebruikt moet worden(!). Voor het ondersteunen van deze functionaliteit wordt in het TC een functie worden geboden waarmee de AP?s bij een school opgevraagd kunnen worden.

In de praktijk houdt de school de huidige AP?s voor de OV (overstap) uitwisseling én krijgt er een of meer AP?s bij voor ieder SWV/Pakket combinatie waarmee de school wil uitwisselen. In het ontvangende RP/SWV systeem is niet bekend voor welk SWV het dossier bedoeld is(!). Omdat het dossier in het schoolgedeelte binnenkomt, zal daar de overdracht naar het correcte SWV worden ingezet.

Bij het starten van een PaO (Passend Onderwijs) uitwisseling moet er in het bron LAS door de eindgebruiker het juiste AP gekozen worden. Het LAS waar de aanvraag gestart wordt, kan bij het TC een lijst opvragen van alle AP?s met doel (nieuw veld) ?PaO? (Passend Onderwijs) van de school. Hiermee kan in het LAS een lijst opgebouwd worden waaruit de schoolmedewerker een AP kiest. Vervolgens kan vanuit het LAS een Notificatie worden verstuurd naar het desbetreffende AP. Via deze Notificatie verkrijgt het SWV-systeem de KoppelSleutel waarmee het Dossier opvraagd kan worden.

Afspraak gegevensset

OSO gegevensset



Binnen OSO is de afspraak OSO gegevensset van toepassing op alle getransporteerde Dossiers. Dit geldt zowel voor de overstapdossiers (OV) tussen scholen als de overdracht ter ondersteuning van aanvragen bij samenwerkingsverbanden passend onderwijs (PaO).

De gegevensset afspraak bestaat uit:

- de beschrijving van de afspraak.
- technische bundel(s)
- codelijsten: codelijsten en toetscodelijst

In de afspraak wordt beschreven voor welk doel en binnen welke kaders de gegevensset mag worden overgedragen. Binnen de OSO gegevensset worden een aantal profielen onderscheiden. Een profiel, zoals het POVO voor de overstap van PO- naar VO-scholen, beschrijft de blokken van velden die toegepast moeten/mogen worden binnen een uitwisseling.
Een technische bundel is de implementatie van een aantal profielen in een schema(xsd) en bijbehorende validatie logica (xslt). In OSO'17 is de validatie logica opgesplitst in een gedeeld deel dat de controle op correct gebruik van (toets)code's controleert én een deel dat de specifieke profielen in een bundel valideert. Door het toegenomen aantal profielen is er gekozen om met een bundel voor OV en een bundel voor PaO profielen te werken.
De codelijsten zijn waardetabellen van in velden gebruikte code's en toetscode's. Vanwege hun hogere update frequentie zijn apart geplaatst en worden apart bijgewerkt en gereleased.
Met het KVS kan een Dossier gevalideerd worden tegen de definities van de gegevensstandaard. In het KVS wordt een Dossier getest tegen het xsd en de xslt van een specifieke versie.

Versies en nummering

Gegevensset

De gegevensset kent eigen versies die zelfstandig, maar in overleg met OSO (infrastructuur), worden beheerd. De OSO gegevensset kent een versie nummer bestaande uit twee delen:

- hoofdversie: jaar (4 digits)
- release versienummer

Bijvoorbeeld: 2017.1

- Een hoofdversienummer geldt doorgaans voor een heel (school)jaar en wordt binnen dit jaar gehanteerd.
- Een release-versienummer wordt opgehoogd wanneer er wijzigingen op veld niveau nodig zijn. Wijzigingen in (toets)code's hebben geen invloed op de release versie.

Bundels

Een technische bundel heeft een versie aanduiding die als volgt is opgebouwd:

- doel van uitwisseling: OV of PaO
- hoofdversie (gegevensset)
- release versienummer (gegevensset)
- datum

De hoofdversie en release-versienummer verwijzen naar de versie van de gegevensset die in de bundel wordt toegepast.
De datum duidt de specifieke bundel aan die op die datum is uitgegeven. Het is mogelijk dat voor eenzelfde combinatie van doel én versie (hoofd en release) van de gegevensset meerdere versies van bundels uitgegeven worden (bijvoorbeeld voor het oplossen van fouten in controles).

Validatieversie

In het KVS (en in aangesloten systemen die Dossiers lokaal valideren) wordt gewerkt met de validatie versie. Deze komt overeen met de bij de validatie toegepaste bundel(xsd en xslt). Deze is opgebouwd uit:

- hoofdversie (gegevensset)
- release versienummer (gegevensset)
- datum (uitgifte technische bundel)

NB: Door de opsplitsing in aparte bundels voor OV en SWV dossiervalidatie, is het mogelijk dat de validatieversie voor deze overdrachten onderling gaat verschillen(!).

Beveiliging

Beveiligingsrequirements

In de OSO keten worden gegevens over leerlingen in het basis- en voortgezet- onderwijs getransporteerd tussen scholen. 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.

De hoofdveiligheidseisen die gelden en de bijbehorende maatregelen voor de OSO overdracht zijn:

- Alleen vertrouwde Systemen mogen gebruik maken van OSO
    - Kwalificatie van Leveranciers van Systemen
    - Identificatie van Systemen door OIN in PKI Overheidscertificaat
    - Sessie uitgifte en controle in TC
    - Logging in TC
- Alleen toegang tot Dossiers voor geautoriseerde gebruikers
    - Kwalificatie van Scholen
    - Beheer door Schoolmedewerkers van Aanleverpunten
    - Versleuteling van het transport van de Dossiers
    - OSO Register voor controle School-Leverancier relatie
    - Logging in Systemen

Kwalificatie Leveranciers

Om toegang te krijgen tot de OSO keten moeten zowel scholen als softwarelevernciers een kwalificatie traject doorlopen.

- Schoolkwalificatie: Dit traject is beschreven op de Overstap Service Onderwijs site.
- Leverancier kwalificatie: Informatie hier over is hier te vinden.

Aangesloten leveranciers

- Overzicht systemen aangesloten op OSO

Certificaten

In OSO wordt gewerkt met zogenaamde 'SAAS certificaten'*; een leverancier wordt geauthenticeerd door zijn PKI Overheid certificaat. Een 'SAAS certificaat' bevat het OIN/HRN van de leverancier, wat doorgaans het KVK nummer van de Leverancier zal zijn. Er zijn twee speciale gevallen van het gebruik van een 'SAAS certificaat' voorzien:

- De Leverancier heeft meerdere systemen die aangesloten worden op OSO én binnen het OSO verkeer onderscheiden moeten worden. In dit geval moet de betreffende Leverancier per systeem een certificaat aanmaken, waarbij in het OIN veld de optioneel postfix ('001', '002', etc.) wordt toegevoegd.
- Een School werkt met een eigen (instantie van) een schoolsysteem. Een voorbeeld hiervan is wanneer een School zelf een pakket huurt/koopt en in een eigen 'private cloud' omgeving host. In dat geval kan het certificaat van de Leverancier NIET wordt gebruikt en moet de School zelf een certificaat inbrengen.

*Een betere naam zou 'SAAS instantie certificaat' zijn, maar deze naamgeving is ondertussen breed ingeburgerd.

Register

Het register is een onderdeel van het Traffic Center. Het bevat alle registraties van, en koppelingen tussen Leveranciers, Scholen* en Aanleverpunten. Het register wordt gevoed door OfficeHeart en mijnOSO. De volgende punten zetten de rol van het register uiteen. Het register houdt bij:

- Scholen
  - Registratie van het BRIN, naam en de sector waarin de School actief is en of de school gekwalificeerd is voor OSO
- Leveranciers
  - Registratie van het OIN/HRN en de naam van de Leverancier waaronder deze binnen OSO bekend is
- Aanleverpunten:
  - Registratie van de internetlocatie (URL) waarop een schoolsysteem bereikt kan worden. Met de Aanleverpunt registereren aanroep kan deze vanuit het Schoolsysteem worden beheerd.
  - Registratie van welke Leverancier namens een School mag optreden. Vanuit mijnOSO kan een Schoolbestuurder de Aanleverpunten van de School beheren. In het Register wordt per Aanleverpunt opgeslagen welk Systeem (Leverancier) dit Aanleverpunt 'implementeert'.
- Beheren Aanleverpunten. Bij het invoeren van een Aanleverpunt in mijnOSO worden de volgende velden geregistreerd:
  - BRIN van de School (deze wordt vanuit OfficeHeart ingevoerd door Kennisnet, een schoolbestuurder kan deze waarde niet zelf beheren)
  - Aanleverpunt-index (APindex). Een doortellend numeriek veld dat geen eigen betekenis heeft. Samen met de BRIN vormt de APindex een unieke combinatie die een Aanleverpunt identificeert.

    - Een tekstlabel, dit wordt deels vast ingevoerd (BRIN en APindex) en is deels een vrij veld voor het aangeven van bruikbare informatie ("Aanleverpunt voor vestiging X")
- Aanleverpunten in Schoolsystemen. Een Aanleverpunt wordt beheerd in mijnOSO en vastgelegd in het Register. In het Schoolsysteem moet overeenkomend met de informatie in het Register het Aanleverpunt worden aangemaakt. De eigenaar van de Schoolaccount op mijnOSO moet daarbij de informatie over het Aanleverpunt doorgeven aan de eindgebruiker in het Schoolsysteem die het Aanleverpunt beheert.
- Registreren URLs bij Aanleverpunten. De url voor het Aanleverpunt wordt *niet* via mijnOSO beheerd, maar vanuit het Schoolsysteem ingesteld door de registreerURL aanroep. Op het moment dat een Schoolsysteem deze aanroep uitvoert, controleert het Traffic Center of het aanroepende systeem in het Register geregistreerd is als het systeem bij dit Aanleverpunt. Alleen als dit het geval is, wordt de aanroep geaccepteerd.

*'School' kan hier slaan op de instelling, (hoofd)vestiging of administratieve eenheid.

Controles binnen het proces

- Account beheer mijnOSO. Tijdens het School-kwalificatie traject wordt vastgelegd namens welke school (BRIN(4)) een bestuurder mag optreden in mijnOSO.
- Aanleverpunt invoer. Het aanmaken van nieuwe Aanleverpunten wordt telefonisch ondersteund vanuit Kennisnet. In mijnOSO kan een eindgebruiker alleen pakketten van gekwalificeerde Leveranciers kiezen bij een Aanleverpunt.
- AP validatie. Op het moment van aanmaken/beheren van een Aanleverpunt *binnen* een Schoolsysteem vinden twee controles plaats:
    - Op basis van het 'SAAS-certificaat wordt vastgesteld dat de Leverancier toegelaten is op OSO.
    - Op basis van de informatie in de aanroep (BRIN-APindex) wordt vastgesteld of de Leverancier voor dit Aanleverpunt is vastgelegd door de School) in het Register.
- Sessie aanvragen. Bij het aanvragen van een Sessie wordt:
    - Op basis van het 'SAAS-certificaat wordt vastgesteld dat de Leverancier toegelaten is op OSO.
    - Op basis van de informatie in de aanroep (BRIN-APindex) wordt vastgesteld of de Leverancier voor dit Aanleverpunt is vastgelegd door de School) in het Register. **NB**:Een Aanleverpunt mag alleen een dossier opvragen namens de BRIN die bij het Aanleverpunt is vastgelegd(!).
    - In het Register wordt gecontroleerd dat het Aanleverpunt actief is, dat wil zeggen: De School heeft de schoolkwalificatie voor OSO succesvol doorlopen.
    - Er wordt een sessieID toegekend, waarbij door het Traffic Center de combinatie bronBRIN, bronAPindex, zoeksleutel (PGN) wordt vastgelegd.
- Dossier opvragen. Een Bronsysteem valideert of het 'SAAS certificaat' van het aanvragende Bronsysteem valide is.
- Sessie controleren. Een Bronsysteem moet voordat een Dossier wordt uitgeleverd, de aanvraag van het Doelsysteem valideren bij het Traffic Center. Op basis van het sessieID wordt gecontroleerd of de doelBRIN, doelAPindex en zoeksleutel overeenkomen met de bij deze sessieID geregistreerde waarden.

Logs en monitoring

- Logging in TC
- Logging in aangesloten systemen
- Rapportage en monitoring

Uitgangspunten

Doel

OSO wordt gebruikt om de digitale uitwisseling van het leerlinggegevens tussen scholen mogelijk te maken zodat:

- scholen sneller en eenvoudiger beschikken over de informatie over de leerling die relevant is voor het leren en begeleiden van die leerling na een overstap
- de inhoud van het overstapdossier gestandaardiseerd en transparant is voor zowel scholen als leveranciers
- de overdracht van deze persoonsgegevens geschiedt in overeenstemming met de wet- en regelgeving

Basisprincipes

Dataminimalisatie

Scholen zijn zelf verantwoordelijk voor de inhoud van de Dossiers en daarmee ook voor het beperken van die gegevens in het Dossier die nodig zijn voor de vervolgschool. Leveranciers moeten mogelijk maken dat Scholen een Dossier kunnen samenstelling dat voldoet aan deze eis voor doelbinding.

Robuustheid van uitwisseling

In OSO wordt het robuustheidsprincipe gehanteerd, dat (in goed Nederlandsch) luidt: "Be conservative in what you send, be liberal in what you accept."
Praktisch betekent dit dat Bronsystemen voorafgaand aan verzending controleren of een Dossier voldoet aan de correcte versie door deze te valideren bij het KVS of intern. Doelsystemen moeten zo goed mogelijk omgaan met afwijkingen in het ontvangen Dossier.

Proces

Dossier uitwisseling

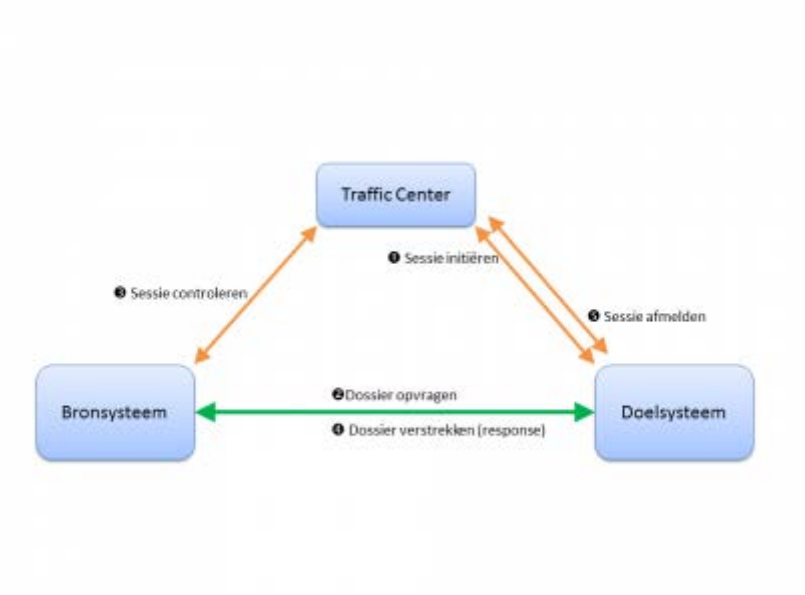
Vanaf OSO'17 worden er twee soorten uitwisselingen ondersteund:

- Overstap tussen Scholen
- Aanvragen bij Samenwerkingsverbanden Passend Onderwijs

In beide typen wordt een dossier uitgewisseld via het basisberichtenverkeer zoals hieronder beschreven. Daarnaast kennen beide varianten hun eigen uitbreidingen hierop:

- Notificatie na Aanvraag (Schooluitwisseling)
- Notificatie met KoppelSleutel (Passend Onderwijs)
- Terugkoppeling naar School (Passend Onderwijs)

Dossier uitwisseling



In de figuur worden de stappen en berichten weergegeven die bij een succesvolle dossier overdracht worden doorlopen. Deze worden hieronder beschreven:

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 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

Binnen één Sessie word per bevraagd Aanleverpunt de berichten .2, .3 en .4 verzonden/ontvangen; deze kunnen meerdere malen binnen één Sessie voorkomen. (Berichten .1 en .5 worden éénmaal per Sessie uitgewisseld.)

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.

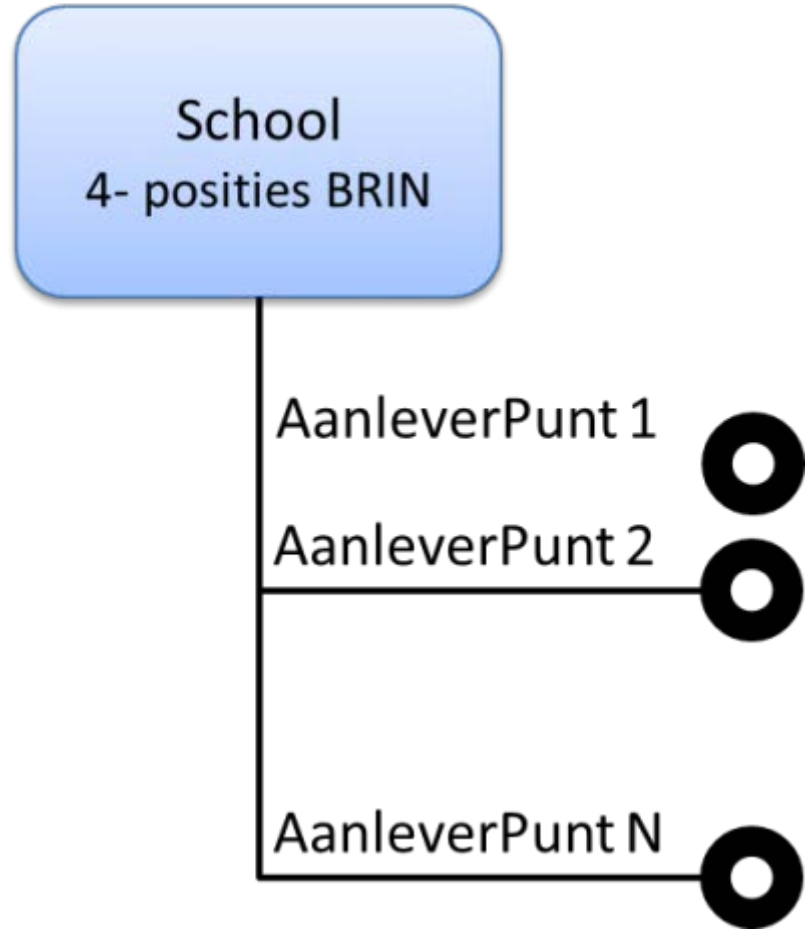
   Dit verzoek bevat het versleutelde BSN en de sessie id uit bericht 2. Het TC controleert deze gegevens; wanneer deze overeenkomen met een uitgegeven nog niet verlopen sessie wordt een ok teruggegeven (SessiecontroleResponse). Controleren sessie

4. Het bronsysteem verstrekt 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 en wordt beschreven in Dossier opvragen.

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

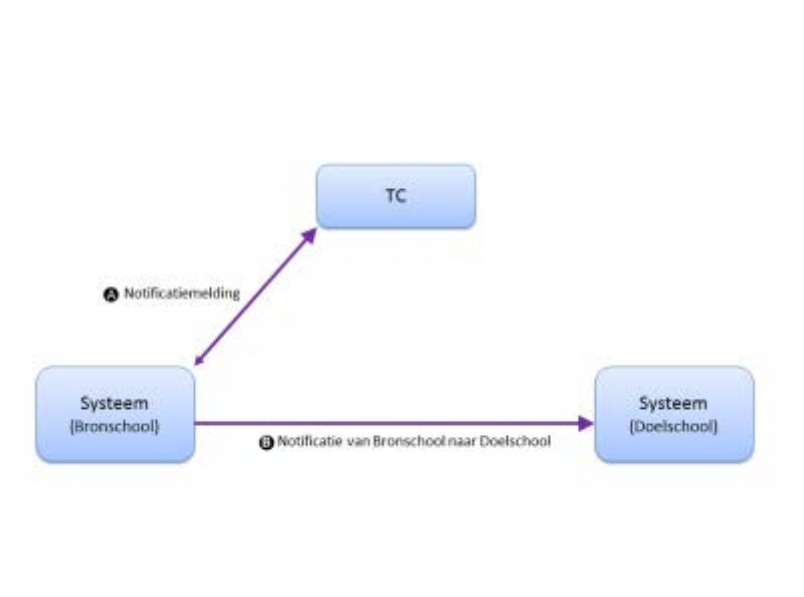
Aanleverpunten



Voor het de uitwisseling van Dossiers via OSO maakt de school gebruik van een of meerdere leerlingadministratiesystemen (LASsen) of regionale platforms (RPs).Een school zelf kan een centrale administratie hebben of deze verspreid hebben opgezet over meerdere vestigingen. Per vestiging kunnen dan ook een of meerdere systemen gebruikt worden
.

Het koppelvlak van een schoolsysteem met OSO een Aanleverpunt (AP). Via het AP wisselt een schoolsysteem informatie uit met het TC en andere OSO systemen. Een AP wordt gekoppeld aan de school en (optioneel) een vestiging.

Notificatie na Aanvraag (Schooluitwisseling)



In de figuur worden de stappen en berichten weergegeven die bij een Notificatie na Aanvraag worden doorlopen. Deze worden hieronder beschreven:

- A: Het Bronsysteem meldt een Notificatie bij het Traffic Center. Het Traffic Center controleert of het Aanleverpunt dat de Notificatie moet ontvangen valide is en een url heeft geregistreerd. Als dit het geval is, wordt de url teruggegeven aan het Bronsysteem.
- B: Het Bronsysteem verstuurt de Notificatie (na ontvangst van de url) naar het Aanleverpunt dat het Dossier eerder heeft aangevraagd.

Notificatie met KoppelSleutel (Passend Onderwijs)

In de figuur worden de stappen en berichten weergegeven die bij een Notificatie met Koppelsleutel worden doorlopen. Deze worden hieronder beschreven:

- A: Het Bronsysteem (LAS) initieert een Notificatie bij het Traffic Center. Het Traffic Center controleert of het Aanleverpunt dat de Notificatie moet ontvangen valide is en bij dezelfde school is geregistreerd(BRIN). Als dit het geval is, wordt en een nieuw gegenereerde KoppelSleutel én de url teruggegeven aan het Bronsysteem.
- B: Het Bronsysteem verstuurt vervolgens de Notificatie met Koppelsleutel naar het Aanleverpunt. Het Doelsysteem start vervolgens een Dossier uitvraag met behulp van de Koppelsleutel.

Push en Pull

In OSO is sprake van een 'pull mechanisme' waarbij de Doelschool het initiatief neemt voor het opvragen van een Dossier bij de Bronschool. De Doelschool heeft daarbij het PGN van het desbetreffende Dossier nodig. Dit verkrijgt de Doelschool buiten OSO om bij de aanmelding/inschrijving van een leerling bij de Doelschool.

In OSO'17 worden Samenwerkingsverbanden Passend Onderwijs aangesloten op OSO. In dit uitwisselproces is sprake van een 'push', waarbij de Bronschool het initiatief heeft. In het LAS van een School wordt een Dossier aangemerkt voor verzending naar een Samenwerkingsverband. Hierna wordt via een Notificatie een Koppelsleutel naar het Samenwerkingsverband systeem (SWV of RP) verstuurd (de PGN mag voor deze overdracht niet gebruikt). Met behulp van de KoppelSleutel wordt het Dossier vervolgens opgevraagd bij de Bronschool.

Sleutel tussen Systemen

In OSO wordt gebruik gemaakt van twee typen sleutels om Dossiers tussen verschillende systemen aan te duiden. De eerste is de 'Zoeksleutel', een sleutel gebaseerd op een gecodeerde versie van het PGN van het Dossier. De tweede is de 'KoppelSleutel', een aanduiding die wordt verstrekt door het TC aan het bronsysteem en via een notificatie naar het doelsysteem verstuurd.

Zoeksleutel

In OSO wordt het Persoonsgebonden Nummer (PGN) toegepast als 'key' voor het Dossier. De PGN is of het BSN of het Onderwijsnummer van de leerling. Bij aanroepen van het TC wordt het PGN versleuteld doorgegeven in het Zoeksleutel veld.
De Zoeksleutel kan door Systemen **niet** ontsleuteld worden (de Key is niet bekend bij deelnemende systemen).

De Zoeksleutel wordt door het Doelsysteem aangemaakt bij het aanvragen van de Sessie. Vervolgens wordt de Zoeksleutel via het DocumentRequest van Doel- naar Bron- systeem verstuurd. Het Bronsysteem stuurt de Zoeksleutel mee met de SessieControle.

KoppelSleutel

De Koppelsleutel wordt in plaats van de Zoeksleutel gebruikt bij de uitwisselingen in het kader van de aanvragen bij Samenwerkingsverbanden Passend Onderwijs. De KoppelSleutel wordt aan het Bronsysteem verstrekt door het TC bij het melden van een Notificatie. Via de Notificatie wordt deze dan doorgeven aan het Bronsysteem.
Een Koppelsleutel is uniek en alleen geldig voor de specifieke uitwisseling en terugkoppeling(en) van:

- Bron Aanleverpunt
- Dossier
- Doel Aanleverpunt

Uitwisselen PaO berichten

De gegevensuitwisseling via OSO tussen scholen en samenwerkingsverbanden Passend Onderwijs (SWV's) ondersteunt het proces van aanvragen van regelingen bij een SWV. Hiervoor zijn er in OSO twee twee mechanismen:

- versturen Dossiers vanuit een LAS naar een RP of SWV.
- versturen terugkoppeling vanuit RP/SWV naar LAS.

Versturen Dossier tbv Aanvraag

In vergelijking met een 'normale' Dossier overdracht tussen scholen geldt dat er voor OSO twee belangrijke verschillen zijn voor deze overdracht:

- PGN mag niet toegepast worden
- initiatief ligt bij verzender (Push ipv Pull)

De 'Notificatie met Zoeksleutel' lost deze twee problemen op . Door het notificatie mechanisme uit te breiden met een alternatieve aanduiding van het dossier, de koppelsleutel, kan het bronsysteem een notificatie sturen naar het doelsysteem, waarna het doelsysteem mbv de koppelsleutel een dossier op kan vragen.
De Koppelsleutel is een random identificatie kenmerk, alleen bekend en geldig voor één specifiek dossier bij twee betrokken systemen. De koppelsleutel is NIET gebaseerd op het PGN of ander persoonskenmerk.

Proces

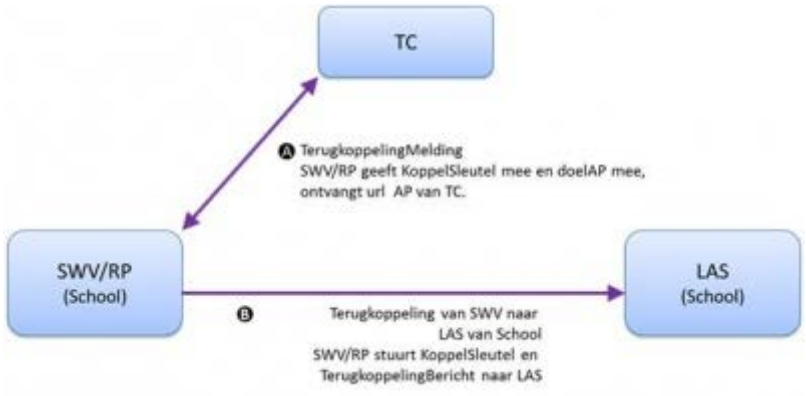
Het versturen van een Dossier met een KoppelSleutel verloopt in twee stappen:

- Bij het melden van een Notificatie geeft het TC de KoppelSleutel terug (samen met de url van het SWV/RP AP). Het LAS verstuurt vervolgens de Notificatie met daarin de KoppelSleutel naar het SWV/RP.

- Het SWV/RP vraagt vervolgens op basis van de KoppelSleutel het Dossier automatisch(!) (zonder tussenkomst van de eindgebruiker) op bij het LAS.

Opgevraagde Dossier(s) worden aan de eindgebruiker in het SWV/RP getoond. De eindgebruiker kiest vervolgens of een Dossier gebruikt zal worden voor het doen van een aanvraag bij het SWV. De verdere afhandeling van deze aanvraag vindt plaats binnen het SWV/RP en valt buiten de scope van OSO(!).

Versturen Terugkoppeling over Aanvraag



De Terugkoppeling geeft informatie over de status van een aanvraag terug vanuit een SWV/RP naar het oorspronkelijke bron LAS. Hiervoor wordt de Koppelsleutel 'herbruikt' die het LAS voor het versturen van het Dossier had ontvangen van het TC. De Terugkoppeling verloopt in twee stappen:

- Melden Terugkoppeling bij het TC
- Versturen daadwerkelijke Terugkoppeling.

De inhoud van een Terugkoppeling bestaat uit de volgende velden:

- KoppelSleutel
- Datum: Moment van verzenden terugkoppeling
- Status (optioneel): Een vrij tekst veld dat de status van de aanvraag beschrijft (?In behandeling?, ?TLV toegekend?, ..)
- RegelingNummer (optioneel): Een vrij tekst veld waarin een verwijzing naar een (toegekende) regeling, arrangement of anders kan worden meegegeven.

- Toelichting (optioneel): Een vrij tekst veld waarin een toelichting bij de terugkoppeling kan worden gevoegd.
- Bijlage(n)(optioneel): Bestand(en) kunnen aan de terugkoppeling worden toegevoegd (Hiervoor gelden dezelfde limieten als voor bijlagen in een OSO dossier).

De velden in de Terugkoppeling zullen (nog) niet worden gestandaardiseerd en zijn ook niet bedoeld om acties in het ontvangende systeem te trigger?en. Ze zijn ?human readable? en bedoelt om als ?oplegger/post it? aan/bij een Dossier getoond te worden in het LAS.

NB1: Een Koppelsleutel kan gebruikt worden voor het sturen van meerdere Terugkoppelingen. Het kan zijn dat voor één Dossier meerdere Koppelsleutels bekend zijn. OSO stelt geen eisen aan het omgaan met de processen die tussen LASsen en RP's/SWV's worden ingericht tbv Passend Onderwijs.
NB2: LASsen die deze functie niet ondersteunen moeten deze wel implementeren en een ?Operatie niet ondersteund? terug geven wanneer deze wordt aangeroepen.

Registreren Aanleverpunt

Context

In het Register wordt per School bijgehouden welke Aanleverpunten bekend zijn. Een Schoolmedewerker kan via 'MijnOSO' Aanleverpunten aanmaken en beheren. Als een Aanleverpunt is aangemaakt kan de Schoolmedewerker die in het Schoolsysteem registreren. Via de Aanleverpunt registratie wordt een Aanleverpunt in het Register 'gekoppeld' aan een Aanleverpunt zoals dat in een Schoolsysteem is aangemaakt. Daarnaast wordt via deze aanroep vanuit het Schoolsysteem de correct url van het Aanleverpunt ingesteld. Zowel Bron- als Doel- systemen moeten hun Aanleverpunten registreren. (Bronsystemen kunnen zonder registratie geen Notificatie ontvangen).

Leveranciers kunnen ervoor kiezen om deze aanroep te combineren met het valideren van de invoer bij een Aanleverpunt.

Basisscenario

1. Een Schoolsysteem verstuurt een registreer Aanleverpunt request naar het Traffic Center.
2. Het Traffic Center controleert of het Aanleverpunt bekend is in het Register en of het Schoolsysteem gemachtigd is om de url van dit Aanleverpunt te registreren.
3. **If** Aanleverpunt geregistreerd mag worden
    1. Het Traffic Center registreert het Aanleverpunt in het Register
4. **Else**
    1. Aanleverpunt verstuur foutmelding aan Schoolsysteem

- Request

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:ns="http://xml.eld.nl/schemas/Overstapservice/20170401">
   <soapenv:Header/>
   <soapenv:Body>
      <ns:registrerenAanleverpuntRequest>
         <ns:aanleverpuntIndex>1</ns:aanleverpuntIndex>
         <ns:brin>12SS</ns:brin>
         <ns:url>https://aanleverpunturl.nl</ns:url>
      </ns:registrerenAanleverpuntRequest>
   </soapenv:Body>
</soapenv:Envelope>
```

- Response:

```
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/20170401">
         <over:resultaat>RegistratieGelukt</over:resultaat>
      </over:registrerenAanleverpuntResponse>
   </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Overzicht meldingen

Resultaat	**Type flow (N, A, E)**	**Omschrijving**
RegistratieGelukt	N	De URL is geregistreerd voor het aanleverpunt
SchoolOnbekend	E	Het gebruikte certificaat correspondeert met het BRIN-nummer en aanleverpunt in de registreerAanleverpuntRequest, echter het BRIN-nummer is niet bekend in het Traffic Center. Dit scenario kan voorkomen indien een school is gedeactiveerd in het Traffic Center.
AanleverpuntNietBekend	A	Aanleverpunt (BRIN + APindex) is niet bekend bij het Traffic Center
OngeautoriseerdAanleverpunt	E	De aanleverpuntcode in het gebruikte certificaat correspondeert niet met het aanleverpunt in het registreerAanleverpuntRequest. Het bronsysteem probeert een een URL te registreren voor een aanleverpunt met een certificaat dat bedoeld is voor een ander aanleverpunt.
OngeldigeURL	E	De URL die meegegeven werd in het registreerAanleverpuntRequest is niet valide.

Ping Traffic Center

Context

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. 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.

Basisscenario

1. Een Schoolsysteem 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.

- Exceptions:

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.

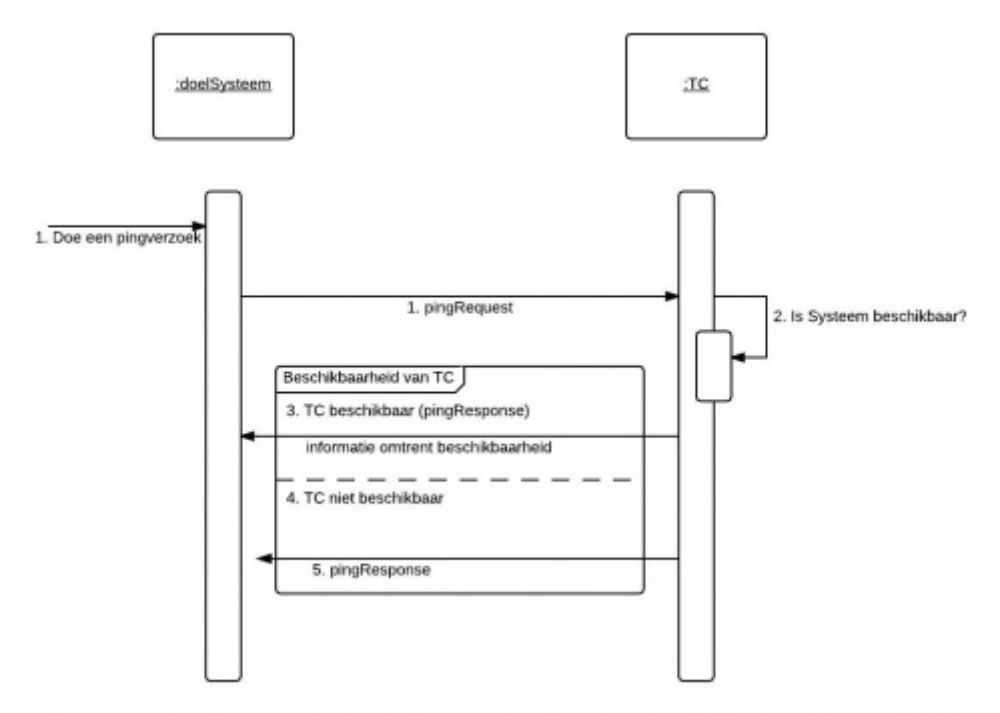
- Request:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:ns="http://xml.eld.nl/schemas/Overstapservice/20170401">
   <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/20170401">
         <over:available>true</over:available>
         <over:applicationVersion>snapshot</over:applicationVersion>
         <over:systemTime>2017-02-23T09:34:36.695+01:00</over:systemTime>
      </over:pingResponse>
   </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Sequence Diagram Ping Service



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).

Controleren Aanleverpunt

Context

Bij het invoeren van Aanleverpunten in Schoolsystemen kunnen eindgebruikers fouten maken bij het invoeren van de gegevens, die overeen moeten komen met de gegevens van het desbetreffende Aanleverpunt in het Register. De Aanleverpunt-sleutel (APsleutel) biedt een mogelijkheid de invoer van de gebruiker te controleren. De ?sleutel-controle? bewaakt de correcte combinatie van Leverancier (via het SAAS certificaat), BRIN en AP-index. De ?sleutel-controle? biedt geen extra beveiliging of juridische zekerheid(!).

Deze aanroep mag door een Leverancier worden toegepast, deze is **niet verplicht**(!).* Als een Leverancier deze aanroep implementeert, dan **moet** deze worden uitgevoerd *voorafgaand* aan het registeren van een Aanleverpunt.

NB: In OSO'17 is de optionele parameter 'doel' aan deze aanroep toegevoegd. Als deze parameter niet wordt meegeven vanuit het schoolsysteem, wordt de waarde 'OV' veronderstelt; de waarden 'OV' of 'PaO' kunnen als geldige waarde worden meegegeven. Met deze uitbreiding is in het schoolsysteem vast te stellen of ook het doel van het Aanleverpunt correct is ingevoerd.

In OSO'16 is gekozen voor het optioneel toepassen van een AP sleutel na discussies in het Technisch Overleg en op de mailinglijst (Zie Bestand:Uitbreiding OSO functionaliteit met APvalidatie 20160210.pdf en Bestand:Uitbreiding OSO functionaliteit met APvalidatie 20160216 def.pdf voor meer informatie.) Daarbij wordt er gewerkt met een 'random' betekenisloze sleutel.

*De aanroep maakt wel onderdeel uit van de WSDl om te voorkomen dat er met meerdere WSDL's moet worden gewerkt.

Basisscenario

1. Een Schoolsysteem verstuurt een APsleutel Controle request naar het Traffic Center.
2. Het Traffic Center controleert of de waarden van BRIN, APindex én Doel voor het Aanleverpunt correct zijn
3. **If** waarden correct
    1. Het Traffic Center controleert of Leverancier (OIN uit certificaat) overeenkomt met geregistreerde Leverancier
    2. **If** Leverancier (OIN uit certificaat) overeenkomt met geregistreerde Leverancier
        1. Het Traffic Center controleert of APsleutel waarde overeenkomt met waarde in Register
        2. **Íf** waarde correct
            1. Traffic Center geeft bevestiging dat de APsleutel is gecontroleerd
        3. **Else**
            1. Traffic Center verstuurt foutmelding over incorrecte APsleutel
    3. **Else**
        1. Traffic Center verstuurt foutmelding over niet geautoriseerde Leverancier
4. **Else**
    1. Traffic Center verstuurt foutmelding over BRIN/APindex aan Schoolsysteem

Request

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:ns="http://xml.eld.nl/schemas/Overstapservice/20170401">
   <soapenv:Header/>
   <soapenv:Body>
      <ns:controlerenAanleverpuntsleutelRequest>
         <ns:brin>12SS</ns:brin>
         <ns:aanleverpuntIndex>1</ns:aanleverpuntIndex>
         <ns:aanleverpuntSleutel>790F584E-59F9-449A-8BA3-
77AE315721F4</ns:aanleverpuntSleutel>
      </ns:controlerenAanleverpuntsleutelRequest>
   </soapenv:Body>
</soapenv:Envelope>
```

Element	Uitleg	Opmerkingen
BRIN	Dit is het brinnummer van de School waar de AP's onder geregistreerd zijn.	Verplicht. BRIN(4) wordt hier gebruikt (in lijn met sessie aanvraag).
aanleverpuntIndex	'001', '002', etc.	Verplicht. Duidt samen met BRIN het specifieke Aanleverpunt aan dat gecontroleerd wordt.
Doel	OV (overstap) of PaO (Passend Onderwijs)	Optioneel. Wanneer deze parameter niet wordt meegegeven wordt de waarde 'OV' toegepast door het TC.
APsleutel	Unieke sleutel zoals gegenereerd in OfficeHeart/mijnOSO bij het aanmaken van een AP.	Optioneel.

Response

```
<SOAP-ENV:Envelope xmlns:SOAP-
ENV="http://schemas.xmlsoap.org/soap/envelope/">
   <SOAP-ENV:Header/>
   <SOAP-ENV:Body>
      <over:controlerenAanleverpuntsleutelResponse
xmlns:over="http://xml.eld.nl/schemas/Overstapservice/20170401">
         <over:resultaat>AanleverpuntsleutelCorrect</over:resultaat>
      </over:controlerenAanleverpuntsleutelResponse>
   </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Overzicht meldingen

Code	Resultaat	Omschrijving
AanleverpuntsleutelCorrect	Aanleverpunt bij APsleutel correct	De validatie is succesvol
AanleverpuntsleutelIncorrect		De APsleutel komt niet voor in het Register.
OngeautoriseerdAanleverpunt		Het gebruikte administratiesysteem (herkend aan het OIN uit het PKIoverheid-certificaat) wijkt af het administratiesysteem dat in het register (via MijnOSO) is geregistreerd. Dit treedt bijv. op als een gebruiker een nieuw aanleverpunt (voor een nieuw type administratiesysteem) vanuit een bestaand administratiesysteem probeert te registreren.
AanleverPuntNietBekend		| De opgegeven BRIN-APindex combinatie komt niet voor in het Register bij deze APsleutel
SchoolNietBekend		Het BRIN komt niet voor in het register
DoelNietBekend		Het opgegeven Doel heeft een afwijkende waarde (moet zijn: PaO of OV)

Code	Resultaat	Omschrijving
DoelWijktAf		Het opgegeven Doel (PaO/OV) komt niet overeen met dat in het register

Opvragen Aanleverpunten

Actor(s)	Goal(s)
BronSysteem, DoelSysteem	Overzicht opvragen van actieve Aanleverpunten in OSO.
Traffic Center	Leveren informatie over Aanleverpunten

Basisvariant: Opvragen AP informatie

Met deze aanroep kan (zonder dat daar een Sessie voor nodig is) informatie over Aanleverpunten opgevraagd worden bij het TC. Deze informatie kan voor een aantal zaken gebruikt worden, zoals:

- Beheren AP's in het aangesloten systeem
- Bij het registren van AP's (via de APsleutel kan informatie over het specifieke AP worden opgehaald
- Voor het vullen van de keuzelijst van AP's bij de SWV aanvragen.

NB: Alle filter parameters van deze aanroep zijn optioneel. Door geen parameter in te vullen, wordt een lijst van alle (actieve) AP's die bij het TC bekend zijn opgevraagd. Dit is incidenteel toegestaan, maar het wordt gevraagd en sterk aanbevolen om 'zuinig' met deze functie om te springen.

Preconditie

- Bron/Doelsysteem is toegelaten op OSO keten
- Bron/Doelsysteem heeft geldig *OSO certificaat*

Postconditie

- TC heeft Bron/DoelSysteem overzicht van Aanleverpunten verstrekt

Request

- Zonder filterparameters

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:ns="http://xml.eld.nl/schemas/Overstapservice/20170401">
   <soapenv:Header/>
   <soapenv:Body>
      <ns:overzichtAanleverpuntRequest>
      </ns:overzichtAanleverpuntRequest>
   </soapenv:Body>
</soapenv:Envelope>
```

- Met filter op APsleutel

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:ns="http://xml.eld.nl/schemas/Overstapservice/20170401">
   <soapenv:Header/>
   <soapenv:Body>
      <ns:overzichtAanleverpuntRequest>
      <ns:aanleverpuntSleutel>E7B01291-3DA0-4F68-BD17-
AB74880050B6</ns:aanleverpuntSleutel>
      </ns:overzichtAanleverpuntRequest>
   </soapenv:Body>
</soapenv:Envelope>
```

Element	Uitleg	Opmerkingen
BRIN	Dit is het brinnummer van de School waar de AP's onder geregistreerd zijn.	Optioneel. BRIN(4) wordt hier gebruikt (in lijn met sessie aanvraag).
Sector	PO, VO	Optioneel. Afgeleid van sector 'eigenaar' (school)
Doel	OV (overstap) of PaO (Passend Onderwijs)	Optioneel.
APsleutel	Unieke sleutel zoals gegenereerd in OfficeHeart/mijnOSO bij het aanmaken van een AP.	Optioneel.
Actief		Optioneel. Impliciet

Response

```
<SOAP-ENV:Envelope xmlns:SOAP-
ENV="http://schemas.xmlsoap.org/soap/envelope/">
   <SOAP-ENV:Header/>
   <SOAP-ENV:Body>
      <over:overzichtAanleverpuntResponse
xmlns:over="http://xml.eld.nl/schemas/Overstapservice/20170401">
         <over:brin>
            <over:aanleverpunt>
               <over:brin>17PR</over:brin>
               <over:aanleverpuntIndex>0</over:aanleverpuntIndex>
               <over:sector>PO</over:sector>
               <over:wijzigingsdatum>2013-01-01
00:00:00.0</over:wijzigingsdatum>
               <over:label>17PR00000 LAS PCBS De Wegwijzer</over:label>
               <over:doel>OV</over:doel>
            </over:aanleverpunt>
            <over:aanleverpunt>
               <over:brin>00MS</over:brin>
               <over:aanleverpuntIndex>0</over:aanleverpuntIndex>
               <over:sector>PO</over:sector>
               <over:wijzigingsdatum>2013-01-01
00:00:00.0</over:wijzigingsdatum>
               <over:label>00MS00000 LAS Professor Waterinkschool School
voor SO</over:label>
               <over:doel>OV</over:doel>
            </over:aanleverpunt>
         </over:brin>
      </over:overzichtAanleverpuntResponse>
   </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Uitzonderingen en meldingen

Hieronder worden alternatieve scenario's en de bijbehorende melding opgesomd:

Resultaat	Omschrijving	Toelichting
<Lijst met AP's>	TC retourneert (gefilterde) lijst met Aanleverpunten	*NB: Lijst kan leeg zijn(!)*
DoelNietBekend	Het opgegeven Doel heeft een afwijkende waarde (moet zijn: PaO of OV)	AP's hebben of een Doel 'PaO' of een Doel 'OV'
SectorNietBekend	De opgegeven Sector heeft een afwijkende waarde	Sector moet een geldige onderwijssector zijn (PO, VO, ..)
<Geen response>	Technische fout	Het bronsysteem staakt het opvragen van de Aanleverpunten.

Samenstellen Dossier

Context

Voorafgaand aan verzending wordt een Dossier samengesteld door Medewerker(s) van de Bronschool. Zij dragen er zorg voor dat de gegevens correct en actueel zijn. Ook moet vooraf de inzage/toestemming door ouders of leerling van het Dossier hebben plaatst gevonden. *In OSO'16 wordt bijgehouden wanneer een medewerker van de Bronschool een Dossier 'gereed' verklaard (Verzameldatum). Deze wordt gebruikt om vast te stellen of een Dossier is gewijzigd sinds de vorige opvraag.*

Het samenstellen van het Dossier is een use case die zich buiten de scope van OSO plaats vindt. Het samenstellen van het Dossier vindt plaats voorafgaand aan de overdracht en staat daar verder los van.Het PvE specificeert niet hoe een Bronsysteem 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 juist in deze stap belangrijke eisen en randvoorwaarden gelden waaraan voldaan moet worden bij versturen van een Overstapdossier via OSO.

Bij het samenstellen van het dossier gelden een aantal belangrijke uitgangspunten en randvoorwaarden waar rekening mee moeten worden gehouden. De belangrijkste daarvan is:
De verzendende school is verantwoordelijk voor de inhoud van het verzonden dossier en dient de inhoud per geval te beschouwen.
OSO verzorgt het transport van het Dossier; de inhoud van het dossier wordt bepaald door de verzendende school. Omdat het hier vaak om gevoelige gegevens gaat, dient dit transport veilig plaats te vinden. Daarnaast dient de overdracht aan wettelijke eisen te voldoen.

Onderliggende use cases

- Selectief samenstellen van het Dossier Eindgebruikers van Bronsystemen kunnen de samenstelling van het Dossier aanpassen door 'blokken' van velden uit te schakelen ('opt out').
- Laten inzien dossier Na het samenstellen van het Dossier en voorafgaand aan verzending moet er in de meeste gevallen inzage plaats vinden.
    - Registreren inzage en/of toestemming Een Bronsysteem moet deze inzage registreren in het Dossier.
- Controleren formaat van het dossier Binnen OSO worden de afspraken van de [edustandaard.nl/standaarden/afspraken/afspraak/oso-gegevensset/|Gegevensset OSO] toegepast op de inhoud en vorm van Dossiers. Voorafgaand aan verzending controleert een Bronsysteem of het Dossier hieraan voldoet.

Wettelijke eisen

Dataminimalisatie

Scholen moeten zorgen dat er niet meer gegevens worden over gedragen in het overstapdossier dan noodzakelijk voor het doel van de overdracht nodig 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.

Inzage en toestemming

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. Dit onderwerp staat hier apart beschreven:inzage en toestemming

Aanvullende eisen

Validatie tegen OSO standaard voorafgaand aan verzenden

Voorafgaand aan verzending moet het Bronsysteem valideren dat het Dossier voldoet aan de dossierspecificatie van OSO.

Registreren Verzameldatum

Bronsystemen dienen bij te houden wanneer een Dossier voor het laatst is aangepast.

Uitvoeren Inzage

De verzendende school (bronschool) moet voorafgaand aan verzending, controleren of ouders inzage hebben gehad in het dossier. Alleen als in het dossier is aangegeven dat dit is ingezien door de ouders, mag er tot levering worden overgegaan.
Als er sprake is van een uitwisseling binnen dezelfde school gelden deze eisen niet.
Uitwisselingen binnen dezelfde instelling zijn toegestaan zonder deze inzage. Er is dan geen sprake van 'externe werking' door een andere rechtspersoon. De OSO-term voor een overdracht binnen een school, dus tussen aanleverpunten met een zelfde BRIN, is een 'binnenBRIN'-overdracht. Een voorbeeld hiervan is het overdragen van een dossier van een LAS naar het RI-platform van dezelfde school.
Hetzelfde geldt voor de uitwisseling met een Samenwerkingsverband Passend Onderwijs. Hierbij wordt het Dossier verstuurd naar het School deel in het systeem (RP of SWV) van het Samenwerkingsverband en blijft dus binnen het BRIN(gezag).

Kort samengevat:

- Een bronsysteem mag een dossier pas overdragen als de leerling (indien meerderjarig) of zijn wettelijk vertegenwoordiger(s) het dossier ingezien hebben (PO).

- Een bronsysteem mag een dossier pas overdragen als de leerling (indien meerderjarig) of zijn wettelijk vertegenwoordiger(s) het dossier ingezien hebben en 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, 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!

Hieronder zijn de verschillende type overstappen weergegeven, met de daarbij gestelde eisen:

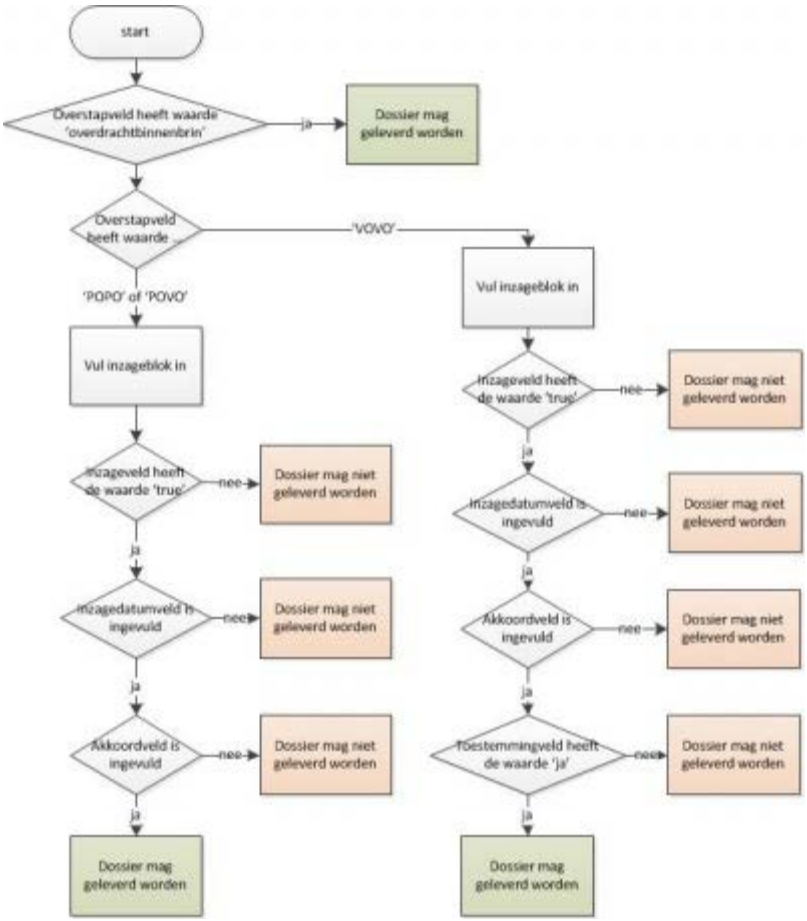
Type overstap	Eisen	Opmerkingen
PO-PO	Oudertoestemming is verplicht	
PO-VO	Ouderinzage is verplicht	
VO-VO	Oudertoestemming is verplicht	In het geval van een VOVO-uitwisseling dient de verzendende school voorafgaand aan de verzending te controleren of de ouders toestemming hebben gegeven voor het verzenden van het dossier. Alleen als in het dossier is aangegeven dat de ouders toestemming hebben gegeven voor de verzending, mag er tot levering worden overgegaan.
overdrachtbinnenbrin	Ouderinzage 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.

NB: Er is verschil tussen akkoord voor inhoud en toestemming 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.
- Toestemming voor verzending is van belang in het VO; hier dient toestemming te zijn gegeven voor de verzending voordat een dossier mag worden verstuurd.

Inzage en toestemming en de OSO-gegevensset

In de OSO gegevensset zijn velden opgenomen voor het registreren van de Inzage en toestemming [edustandaard.nl/standaarden/afspraken/afspraak/oso-gegevensset/]. Hieronder staat ter illustratie een schematische voorstelling van inzage en toestemming, waarbij tags uit de OSO-gegevensset zijn gebruikt.


start
Overstapveld heeft waarde 'overdrachtbinnenbrin'
ja
Dossier mag geleverd worden
Overstapveld heeft waarde
'VOVO'
'POPO' of 'POVO'
Vul inzageblok in
Vul inzageblok in
Inzageveld heeft de waarde 'true'
nee
Dossier mag niet geleverd worden
ja
Inzagedatumveld is ingevuld
nee
Dossier mag niet geleverd worden
ja
Akkoordveld is ingevuld
nee
Dossier mag niet geleverd worden
ja
Dossier mag geleverd worden
Inzageveld heeft de waarde 'true'
nee
Dossier mag niet geleverd worden
ja
Inzagedatumveld is ingevuld
nee
Dossier mag niet geleverd worden
ja
Akkoordveld is ingevuld
nee
Dossier mag niet geleverd worden
ja
Toestemmingveld heeft de waarde 'ja'
nee
Dossier mag niet geleverd worden
ja
Dossier mag geleverd worden

Registreren Inzage

Actor(s)	Goal(s)
Medewerker (Bronschool)	Registeren van moment en uitkomst van inzage dossier
Ouders/verzorgers (van Leerling)	Controleren van inhoud van Dossier

Context

Onderdeel van *Laten inzien Dossier*

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.

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 voor verzending wordt gegeven, toch verzonden worden.
    - In het geval van VO mag een dossier alleen verzonden worden als er toestemming voor verzending wordt gegeven.

Samenstellen Inhoud Dossier

Belangrijk uitgangspunt bij de overdracht van de overstapdossiers is dat de verschillende gegevensonderdelen (met name de optionele onderdelen), indien relevant, bewust worden toegevoegd aan het dossier. Bij uitstek is hiervoor de docent of mentor eindverantwoordelijk, zo goed mogelijk ondersteund door de software. Dit proces van het samenstellen van een OKR met alleen relevante gegevens, heet selectief uitleveren.

Profielen en Blokken

Velden van uitgeschakelde blokken mogen niet opgenomen worden in het Dossier. (Alle (gevulde) velden van een ingeschakeld blok wel). In de gegevensset wordt in OSO?17 gewerkt met profielen. Een profiel verdeelt de gegevensset in blokken van velden. Per type uitwisseling (POVO, POPO, etc.) wordt aangegeven of een blok verplicht of optioneel is. Eindgebruikers kunnen de samenstelling van een dossier wijzigen door optionele blokken aan of uit te zetten.

Per profiel verschilt de ?optionaliteit? van blokken, de indeling van velden per blok is voor de hoofdprofielen gelijk. Voor de uitwisseling met samenwerkingsverbanden wijkt de indeling af, onder andere omdat hier het PGN niet mag worden uitgewisseld). Blokken zijn niet ?genest?, alle blokken zijn van hetzelfde (hoofd)niveau.

Een school kan optionele blokken van velden uit het dossier verwijderen, zodat deze niet meegestuurd worden. De ontvangende school kan in het dossier zien of blokken bewust uitgezet zijn. Dit wordt door de pdf-viewer (door Kennisnet geleverd) ondersteund; ontvangende systemen zijn niet verplicht dit binnen hun systeem te tonen.

Voor meer informatie zie de Edustandaard OSO site.

Functionele eisen

- Bronsystemen moeten hun eindgebruikers in staat stellen om op basis van het profiel optionele blokken aan of uit te schakelen ('opt out').
- In het 'meta deel' van het Dossier moet het Bronsysteem aangeven welke blokken uitgeschakeld zijn.

Valideren Dossier

Een Bronsysteem controleert voorafgaand aan verzending of het Dossier voldoet aan de OSO. Deze controle bestaat uit twee validatie stappen:

- het dossier dient qua ?vorm? te voldoen aan het specificatie schema; dit wordt gevalideerd tegen de xsd
- de inhoud van het dossier voldoet aan de regels vanuit de afspraakt; dit wordt (beperkt) gevalideerd door de xslt

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

Leveranciers kunnen kiezen uit twee methoden om deze controle uit te voeren; een Bronsysteem dient er één toe te passen:

- externe validatie uitgevoerd door Kennisnet Validatie Service*
- lokale validatie in het eigen systeem.

Bij de lokale validatie variant valideert het Bronsysteem het dossier binnen haar eigen omgeving. Daarbij dient gebruikt te worden gemaakt van de correcte versie van de xsd en xslt. Kennisnet zorgt voor de beschikbaarheid van deze bestanden.

*De KVS voorziening kan ook zal als ?scheidsrechter? en voor testdoeleinden toegepast worden.

Klaarzetten Dossier

Gereed zetten dossier

Actor(s)	Goal(s)
Schoolmedewerker (Bronschool)	Dossier klaar zetten voor verzenden en aangeven welke partijen dit Dossier mogen ontvangen.

Bronssystemen houden bij aan welke Scholen een dossier mag worden uitgeleverd. Alleen als het BRIN van de aanvragende School door de Eindgebruiker is aangegeven als Doelschool, mag het dossier uitgeleverd worden. Een Bronsysteem controleert bij een binnengekomen dossieraanvraag of het BRIN van het aanvragende systeem overeenkomt met een BRIN uit de lijst van scholen die zijn aangegeven als ontvanger.

Een Doelssteem mag een voorselectie van doel-BRINs?s aanbieden aan de eindgebruiker (?meest gebruikte BRIN's?), waar de eindgebruiker uit kiest. Er MOET een gebruikershandeling plaats vinden bij het instellen van het doel (het systeem mag niet automatisch kiezen).

Basisscenario

1. Schoolmedewerker (Bronschool) kiest Dossier om gereed te zetten
2. Bronsysteem voert controle uit op Inzage/Toestemming
3. **If** controle op Inzage/Toestemming akkoord is
    1. Schoolmedewerker geeft Doelscho(o)l(en) aan die Dossier mogen ontvangen (BRIN(4))
    2. Bronsysteem controleert op eerdere aanvragen van Doelsystemen bij aangegeven Doelscholen
    3. **While** er nog openstaande Aanvragen voor Dossier zijn
        1. Bronsysteem verstuurt Notificatie naar Doelsysteem van Aanvraag
    4. Bronsysteem registreert Dossier als 'Gereed voor verzending'
4. **Else**
    1. Bronsyteem geeft melding over nog niet uitgevoerde inzage

Initiëren notificatie

Actor(s)	Goal(s)
Bronsysteem	Melden dat Bronsysteem Notificatie aan Doelsysteem wil versturen en adres van gespecificeerd Aanleverpunt ontvangen.
Traffic Center	Controleren of Notificatie verstuurd kan worden en zorgen dat Notificatie bij juist Aanleverpunt wordt afgeleverd.

Basisvariant: Notificatie voor Dossier overdracht

Een Notificatie wordt verstuurd door Bronsystemen op het moment dat een Dossier klaar wordt gezet, waarvoor eerder een verzoek tot levering van een (of meerdere) Doelsyste(e)men is ontvangen. Een Notificatie wordt altijd naar het specifieke Aanleverpunt dat een verzoek heeft verstuurd geadresseerd. Het versturen van de Notificatie wordt hier verder uitgewerkt.

Basisvariant: Notificatie voor aanvraag bij Samenwerkingsverband

In dit geval wordt de Notificatie gebruikt voor het initiëren van een aanvraag bij een Samenwerkingsverband. Het Dossier wordt ook klaar gezet in het Bronsysteem (maar er is geen eerder verzoek nodig), waarna een specifiek Aanleverpunt door de eindgebruiker moet worden gekozen. De Notificatie wordt alleen naar dit Aanleverpunt verstuurd. Het versturen van de Notificatie wordt hier verder uitgewerkt.

Basis scenario

1. Bronsysteem verstuurt Notificatie Request naar Traffic Center
2. **IF** overdrachtdoel is 'overstapdossier'
    1. **IF** DoelAanleverpunt is actief AND DoelAanleverpunt heeft 'doel' ingesteld op 'OV'
        1. **IF** SessieID is gezet **AND** SessieID is bekend bij TC *
            1. Traffic Center registreert het Notificatie Request
            2. Traffic Center geeft url van het Doelaanleverpunt terug
        2. **ELSE**
            1. Traffic Center geeft foutmelding
        3. **ENDIF**
    2. **ELSE**
        1. Traffic Center geeft foutmelding
    3. **ENDIF**

1. **ELSEIF** overdrachtdoel is 'swv-aanvraag'
    1. **IF** DoelAanleverpunt is actief AND DoelAanleverpunt heeft 'doel' ingesteld op 'PaO'
        1. **IF** SessieID is leeg **
            1. **IF** (BRIN van DoelAP == BRIN van BronAP)
                1. Traffic Center genereert Koppelsleutel
                2. Traffic Center geeft Koppelsleutel en url van het Doelaanleverpunt terug
            2. **ELSE**
                1. Traffic Center geeft foutmelding
            3. **ENDIF**
        2. **ELSE**
            1. Traffic Center geeft foutmelding
        3. **ENDIF**
    2. **ELSE**
        1. Traffic Center geeft foutmelding
    3. **ENDIF**
2. **ENDIF**

*SessieID ingevuld

Notificatie nav eerder verzoek tot levering Dossier. SessieID wordt vergeleken met binnengekomen Sessie Controle verzoeken. Daarbij worden ook gecontroleerd dat de bron-BRIN/APindex én de doel-BRIN/APindex overeenkomen met het originele verzoek waar het sessieID aan werd toegekend.

**Beide parameters leeg

Verzoek om koppelsleutel (Notificatie tbv Aanvraag naar Samenwerkingsverband)

Uitzonderingen en meldingen

Hieronder worden alternatieve scenario's en de bijbehorende meldingen opgesomd:
.

Resultaat	**Omschrijving**	**Toelichting**	***Meldi Eindg***
AanvragerNietBekend	Het bronsysteem (aanleverpunt dat de notificatie meldt) is niet bekend bij het Traffic Center. De aanvrager is niet gerechtigd om de overstapservice te gebruiken.	In het Traffic Center register is de combinatie van bronBrin en bronAanleverpuntIndex niet aanwezig.	De aan is niet gerech de oversta te gebr Neem op met levera
AanvragerAanleverpuntNietBekend	Het bronAanleverpuntIndex is niet geregistreerd voor deze aanvrager (bronBrin).		Het br aanlev niet be het OS systee hierdo geen n meldin worde aangev
AanvragerNietBeschikbaar	De aanvrager (bronBrin) is niet gerechtigd om de overstapservice te gebruiken.		Je sch niet aanges OSO. contac de serv van OS
OngeautoriseerdAanleverpunt	Het OIN van het certificaat komt niet overeen met die van de geregistreerde leverancier. Het bronsysteem (aanleverpunt dat Notificatie meldt) is in het Traffic Center register geregistreerd door een andere leverancier.	Het aanleverpunt (bronBrin/bronAanleverpuntIndex) is bekend bij OSO, maar het aanleverpunt staat geregistreerd bij een andere leverancier.	Interne OSO s Neem op met service van OS
VerstrekkerNietBekend	De verstrekker (het doelsysteem waar de notificatie naartoe verstuurd moet worden) is		Het aanlev van de waarm wilt

Resultaat	Omschrijving	Toelichting	***Meldi Eindg***
	niet bekend bij het Traffic Center.		uitwiss nog ni bekend OSO. contac de betr school
VerstrekkerAanleverpuntNietBekend	Het meegegeven aanleverpunt is niet geregistreerd voor deze verstrekker. Het opgegeven Aanleverpunt (DoelBRIN/APindex) van het Doelsysteem is niet bekend.	Het opgegeven Aanleverpunt van het Doelsysteem is (nog) niet opgenomen in het Register.	Het aanlev van de waarm wilt uitwiss nog ni bekend OSO. contac de betr school
VerstrekkerNietBeschikbaar	De verstrekker is niet gerechtigd om de overstapservice te gebruiken. Het opgegeven Aanleverpunt van het Doelsysteem is (nog) niet gerechtigd om de overstapservice te gebruiken.	De Doelschool is bekend in het Register, maar het opgegeven Aanleverpunt is (nog) niet actief. Dit kan bijvoorbeeld veroorzaakt worden doordat de URL van dit Aanleverpunt niet (goed) is geregistreerd	De sch waarm wilt uitwiss heeft g actieve aanlev bij OS contac de betr school
SessieIDNietBekend	Het opgegeven SessieID is niet bekend in de log van het Traffic Center.	Het SessieID dat de BronSchool opgeeft is niet opgeslagen als geldig SessieID bij het Traffic Center.	Er hee een int fout voorge tijdens melder notific Neem op met softwa leveran
OVnotificatieIncorrect	De overdrachtdoel is 'overstapdossier' maar SessieID en/of Aanvraagdatum zijn niet ingevuld.	Voor een Notificatie zijn een eerder toegekend SessieID en Aanvraagdatum nodig.	Er hee een int fout voorge tijdens melder

Resultaat	Omschrijving	Toelichting	***Meldi*** ***Eindg***
			notific Neem op met softwa leverar
OVnotificatieAPIncorrect	Het doel is 'OV' ('overstapdossier') maar de bronAP heeft als doel 'PaO' of de doelAP heeft als doel 'PaO' ('Samenwerkingsverband')	Een Notificatie met als doel 'overstapdossier' gespecificeerd mag niet naar AP's van type 'OV' worden verstuurd, maar kan alleen naar AP's van type 'LAS' of 'RP' worden verstuurd.	Er hee een int fout voorge tijdens melder notific Neem op met softwa leverar
SWVnotificatieAPIncorrect	Het doel is 'swv-aanvraag' maar de de bron AP heeft als doel 'LAS'' of de doelAP heeft als doel 'LAS'	Een Notificatie met doel 'overstapdossier' kan alleen naar AP's van type 'PaO' of 'RP' verstuurd.	Er hee een int fout voorge tijdens melder notific Neem op met softwa leverar
SWVnotificatieIncorrect	Het doel is 'swv-aanvraag' maar SessieID en/of Aanvraagdatum zijn ingevuld.	Een Notificatie met doel'overstapdossier' kent geen SessieID of Aanvraagdatum.	Er hee een int fout voorge tijdens melder notific Neem op met softwa leverar
SWVnotificatieGeenRelatieMetDoel	Het doel is 'swv-aanvraag' maar de BRIN van de DoelAP wijkt af van de BRIN van de BronAP.	Een Notificatie van het overdrachtdoel 'overstapdossier' mag alleen naar AP's van dezelfde BRIN (school) verzonden worden.	Er hee een int fout voorge tijdens melder notific Neem op met

Resultaat	Omschrijving	Toelichting	***Meldi*** ***Eindg***
			softwa levera
<Geen response>	Technische fout	Het meldende Bronsysteem staakt de verdere Notificatie en geeft de eindgebruiker hierover een foutmelding.	Er kan verbin gemaa worde OSO s Probee later n

Verwerken openstaande verzoeken

Context

Een bronsysteem toont binnengekomen valide verzoeken tot het leveren van een dossier aan de eindgebruiker. Deze moet op basis van de getoonde informatie kunnen besluiten tot het gereedmaken van het dossier en het klaarzetten daarvan voor de doelschool. Voor verzoeken waarbij het Bronsysteem het Dossier niet kon leveren omdat het Dossier niet in de juiste versie van de Dossierstandaard is opgemaakt, moet dit expliciet worden aangegeven in dit overzicht.

Het verwerken van openstaande verzoeken is een use case die zich buiten de scope van OSO plaats vindt. Het PvE specificeert niet hoe een Bronsysteem dit scenario moet ondersteunen, wel worden er e randvoorwaarden en eisen gesteld om het uitwisselproces binnen Scholen zo goed mogelijk te ondersteunen.

NB: Dit scenario geldt niet voor de PaO uitwisseling.

Randvoorwaarden en eisen

Bronsystemen slaan binnenkomende verzoeken tot het leveren van een dossier op. Deze verzoeken moeten door eindgebruikers inzichtelijk zijn, waarbij in ieder geval de overdrachtsverzoeken die voldoen aan onderstaande eisen getoond moeten worden:

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

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:

- pgn (bsn of onderwijsnummer) van de leerling
- BRIN van aanvragende school
- AP-index van de aanvragende school
- datum/tijdstip binnenkomst van aanvraag
- Indien van toepassing: Aangegeven dat het Dossier niet de correcte versie heeft van de Dossierstandaard.

overstap

Preconditie

- BronSysteem is aangesloten op OSO keten
- BronSysteem heeft DocumentRequest ontvangen van Doelsysteem (en SessieID hiervan geregistreerd)
- BronSysteem heeft Dossier klaargezet uit DocumentRequest van Doelsysteem

Postconditie

- Traffic Center heeft Notificatie Melding geregistreerd
- BronSysteem heeft correcte url van Doelsysteem ontvangen

Aanroep en antwoord

- Request:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:ns="http://xml.eld.nl/schemas/Overstapservice/20170227">
   <soapenv:Header/>
   <soapenv:Body>
      <ns:meldenNotificatieRequest>
         <ns:bronBrin>00AH</ns:bronBrin>
         <ns:bronAanleverpuntIndex>18</ns:bronAanleverpuntIndex>
         <ns:doelBrin>12SS</ns:doelBrin>
         <ns:doelAanleverpuntIndex>1</ns:doelAanleverpuntIndex>
         <ns:sessieId>b8b9a132-51ca-4188-8de7-323842336156</ns:sessieId>
         <ns:aanvraagdatum>2016-03-06T14:19:39.977+02:00</ns:aanvraagdatum>
         <ns:doel>OV</ns:doel>
      </ns:meldenNotificatieRequest>
   </soapenv:Body>
</soapenv:Envelope>
```

Element	Uitleg	Opmerkingen
bronBRIN	Dit is het BRINnummer van de Bronschool dat het DocumentRequest heeft ontvangen en een Notificatie naar het Doelsysteem wil sturen.	Verplicht
bronAanleverpuntIndex	Dit is de index van het Aanleverpunt van het Bronsysteem dat het DocumentRequest naar het Bronsysteem heeft verstuurd.	Verplicht
doelBrin	Dit is het brinnummer van het Doelsysteem dat het documentRequest heeft ingediend bij het Bronsyteem.	Verplicht
doelAanleverpuntIndex	Dit is de index van het Aanleverpunt van het Doelsysteem dat de Sessie aanvraagt.	Verplicht

Element	Uitleg	Opmerkingen
sessieId	Het sessieId van het laatste documentRequest dat het bronSysteem van het doelsysteem heeft ontvangen. Dus het sessieId dat de laatste keer gebruikt is bij het opvragen van het dossier.	Verplicht
aanvraagdatum	Het tijdstip van het laatste documentRequest dat door het doelssysteem is gestuurd om het dossier op te vragen. Het bronssysteem heeft dit tijdstip bewaard.	Verplicht
doel	Geeft het doel waarvoor de Notificatie wordt verstuurd.	Verplicht. **Voor deze overdracht moet de waarde 'OV' gebruikt.**

- Response

```
<SOAP-ENV:Envelope xmlns:SOAP-
ENV="http://schemas.xmlsoap.org/soap/envelope/">
   <SOAP-ENV:Header/>
   <SOAP-ENV:Body>
      <over:meldenNotificatieResponse
xmlns:over="http://xml.eld.nl/schemas/Overstapservice/20170227">
         <over:notificatie>
            <over:aanleverpunt>
               <over:code>1</over:code>
               <over:url>https://aanleverpunturl.nl</over:url>
               <over:type>RIS</over:type>
               <over:label>12SS00001 RIS Testschool Triple W ICT
PO</over:label>
            </over:aanleverpunt>
         </over:notificatie>
      </over:meldenNotificatieResponse>
   </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Tonen aanvragen

Tonen ontvangen dossier aanvragen

Bronsystemen slaan binnenkomende 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-index van de aanvragende school (
- datum/tijdstip binnenkomst van aanvraag

aanvraag

Preconditie

- BronSysteem is aangesloten op OSO keten
- Gebruiker Bronsysteem heeft te notificeren Aanleverpunt van Doelsysteem gekozen
- Bronsysteem heeft Dossier klaargezet dat opgehaald moet worden door Doelsysteem
- BRIN van Bron Aanleverpunt is gelijk aan BRIN van Doel aanleverpunt

Postconditie

- Traffic Center heeft Notificatie Melding geregistreerd
- Traffic Center heeft nieuwe KoppelSleutel gegenereerd en doorgegeven aan Doelsysteem
- BronSysteem heeft correcte url van Doelsysteem ontva

Aanroep en antwoord

- Request:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:ns="http://xml.eld.nl/schemas/Overstapservice/20170227">
   <soapenv:Header/>
   <soapenv:Body>
      <ns:meldenNotificatieRequest>
         <ns:bronBrin>00AH</ns:bronBrin>
         <ns:bronAanleverpuntIndex>18</ns:bronAanleverpuntIndex>
         <ns:doelBrin>00AH</ns:doelBrin>
         <ns:doelAanleverpuntIndex>19</ns:doelAanleverpuntIndex>
         <ns:doel>PaO</ns:doel>
      </ns:meldenNotificatieRequest>
   </soapenv:Body>
</soapenv:Envelope>
```

Element	Uitleg	Opmerkingen
bronBRIN	Dit is het BRINnummer van de Bronschool dat het DocumentRequest heeft ontvangen en een Notificatie naar het Doelsysteem wil sturen.	Verplicht
bronAanleverpuntIndex	Dit is de index van het Aanleverpunt van het Bronsysteem dat het DocumentRequest naar het Bronsysteem heeft verstuurd.	Verplicht
doelBrin	Dit is het brinnummer van het Doelsysteem dat het documentRequest heeft ingediend bij het Bronsyteem.	Verplicht

Element	Uitleg	Opmerkingen
doelAanleverpuntIndex	Dit is de index van het Aanleverpunt van het Doelsysteem dat de Sessie aanvraagt.	Verplicht
sessieId	Het sessieId van het laatste documentRequest dat het bronSysteem van het doelsysteem heeft ontvangen. Dus het sessieId dat de laatste keer gebruikt is bij het opvragen van het dossier.	**Voor dit type overdrachtsoort wordt sessieID niet toegepast(!) en mag dit veld niet voorkomen in het request**
aanvraagdatum	Het tijdstip van het laatste documentRequest dat door het doelssysteem is gestuurd om het dossier op te vragen. Het bronssysteem heeft dit tijdstip bewaard.	**Voor dit type overdrachtsoort wordt aanvraagdatum niet toegepast(!) en mag dit veld niet voorkomen in het request**
doel	Geeft het doel waarvoor de Notificatie wordt verstuurd.	Verplicht. **Voor deze overdracht moet de waarde 'PaO' gebruikt.**

- Response

```
<SOAP-ENV:Envelope xmlns:SOAP-
ENV="http://schemas.xmlsoap.org/soap/envelope/">
<SOAP-ENV:Header/>
<SOAP-ENV:Body>
<over:meldenNotificatieResponse
xmlns:over="http://xml.eld.nl/schemas/Overstapservice/20160411">
  <over:aanleverpunt>
    <over:code>102</over:code>
    <over:url>https://aanleverpunturl.nl</over:url>
    <over:type>RP</over:type>
    <over:label>12SS0102 RP Testschool Triple W ICT PO</over:label>
  </over:aanleverpunt>
</over:meldenNotificatieResponse>
</SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Notificeren van Doelsystemen

Context

Na het klaarzetten van een Dossier verstuurt een Bronsysteem een Notificatie naar een Bronsysteem* dat eerder een DocumentRequest voor het specifieke Dossier heeft verstuurd. Voorafgaand aan het versturen van de Notificatie stuurt het Bronsysteem eerst een Notificatiemelding aan het Traffic Center. Het Traffic Center registreert de Notificatiemelding en geeft de actuele url van het Aanleverpunt van het Doelsysteem terug aan het Bronsysteem.

* Het klaarzetten van het Dossier 'triggert' de Notificatie maar staat verder 'los' van deze interactie. Ongeacht of de Notificatie slaagt of niet wordt het 'klaarzetten' uitgevoerd.

Juridische randvoorwaarden

- De Bronschool is verantwoordelijk voor het verzenden van de Notificatie; daarom mag deze alleen verzonden worden als aan de volgende voorwaarden is voldaan:
- Een Notificatie mag alléén verzonden worden als het Doelsysteem dit dossier eerder heeft aangevraagd.
- Notificatie MOET naar het specifieke Doelsysteem dat aanvraag heeft gedaan (niet naar alle Aanleverpunten bij een School)
- Zenden van notificatie moet een ?bewuste gebruikershandeling? in het Bronsysteem zijn. Het zenden mag een onderdeel zijn van het klaarzetten van het dossier. In het laatste geval betekent dit, dat als er in het Bronsyteem met een checkbox voor notificatie wordt gewerkt, het veld niet vooraf al 'aangevinkt' mag zijn. De gebruiker moet zelf het vinkje zetten. Ook moet een duidelijke uitleg worden gegeven welk gevolg het zetten van het vinkje heeft. Dit kan bijvoorbeeld door een vraagteken erachter met een 'mouse over tekst' zoals: "door dit vinkje aan te zetten zet u dit overstapdossier klaar voor de uitwisseling en wordt een notificatie verstuurd aan het Doelsysteem."
- Het opvragen van een dossier op basis van een Notificatie moet (ook) een ?bewuste gebruikershandeling? in het Doelsysteem zijn.

Overige randvoorwaarden

- Notificatie is **verplicht** voor alle typen uitwisseling, met uitzondering voor de binnenBRIN uitwisseling. Bij binnenBRIN uitwisselingen is het Notificeren optioneel.
- De termijn die in OSO ?17 gehanteerd gaat worden voor de geldigheid van documentRequests is **6 (kalender)maanden**. Verzoeken tot Dossier die ouder zijn dan zes maanden mogen **niet** leiden tot Notificaties.
    - Bronsystemen moeten alle documentRequests met een aanvraagDatum tot drie maanden geleden bewaren voor notificatie doeleinden.
    - Bronsystemen mogen geen notificatie versturen op basis van een documentRequest met een aanvraagDatum ouder dan drie maanden.

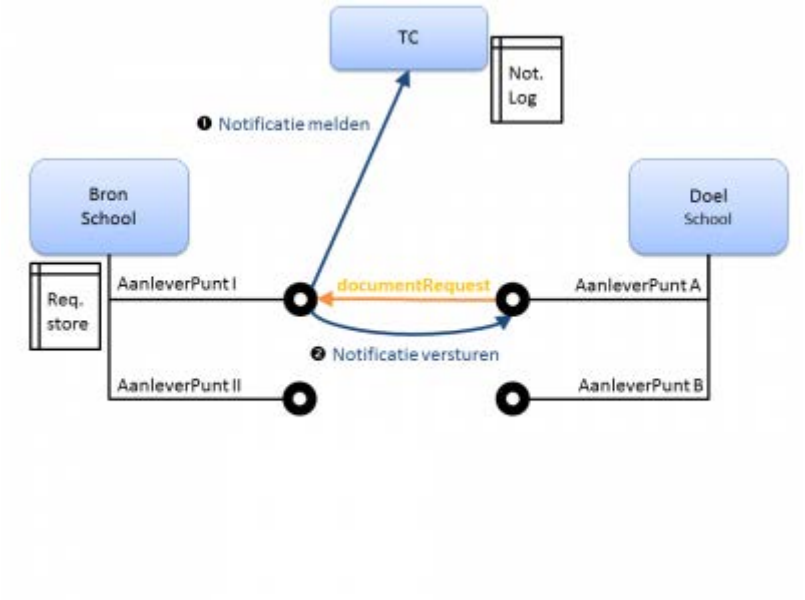
Context

Als een Dossier gereed wordt gezet in een Bronsysteem controleert het Bronsysteem of er aanvagen zijn geweest voor dit Dossier van Doelsystemen die niet zijn uitgeleverd. Als dit het geval is en de Eindgebruiker van het Bronsysteem toestemming geeft, verstuurt het Bronsysteem een Notificatie naar deze Doelsyste(e)men.

Onderliggende use cases

- Notificatie melden
- Notificatie versturen

Notificatie mechanisme



In de figuur worden de stappen en berichten weergegeven die bij een succesvolle Notificatie worden doorlopen. Deze worden hieronder beschreven:

- Een Doelsysteem stuurt een DocumentRequest. Wanneer het Bronsysteem het gevraagde dossier niet kan leveren, wordt de relevante informatie uit het documentRequest opgeslagen door het Bronsysteem.
    - De aanvraagDatum bij het Dossier wordt door het Bronsysteem ingesteld met het tijdstip waarop het (laatste) documentRequest voor dit Dossier werd ontvangen.
    - Als er al een documentRequest voor het desbetreffende dossier is ontvangen, dan wordt de aanvraagDatum bijgewerkt met de datum uit het laatste documentRequest. Ook wordt het sessieID vervangen met het sessieID uit dit laatste Documentrequest.
    - Het sessieID is het sessieID zoals het Doelsysteem die meegeeft in het documentRequest. Dit sessieID wordt door het Bronsysteem doorgegeven aan

het TC bij het melden van de Notificatie en heeft geen ander doel dan bij het loggen van het verkeer door het TC.

- Op het moment dat een bronSysteem een dossier klaarzet voor een doelschool (BRIN(4)) controleert het bronSysteem of er voor dit dossier documentRequests afkomstig zijn geweest van deze doelschool.
    - Meerdere aanleverpunten van een School (BRIN(4)) kunnen documentRequests hebben gestuurd. Voor één dossier wordt maximaal één notificatie naar hetzelfde Aanleverpunt gestuurd.
    - Omdat er documentRequests kunnen zijn van meerdere aanleverpunten onder één BRIN, kan het klaar zetten van een dossier leiden tot meerdere Notificaties.
    - Het Bronsysteem stuurt een Notificatie als de verlooptermijn van het documentRequest niet is verstreken
- Het Bronsysteem vraagt haar eindgebruiker voor een bevestiging voor het versturen van een Notificatie.
- Na bevestiging van de eindgebruiker meldt het Bronsysteem de Notificatie aan het Traffic Center.
    - Het Traffic Center controleert of het Aanleverpunt valide is
    - Het Traffic Center geeft de url van het valide Aanleverpunt terug
- Het bronsysteem verstuurt (na een positieve respons van het TC op het NotificatieMelding) een Notificatie naar het doelsysteem van het aanleverpunt. Het doelsysteem bevestigt de ontvangst.
    - Het bronsysteem doet één poging per notificatie om deze te versturen na het doelsysteem; er volgen geen nieuwe pogingen wanneer de aflevering faalt.
    - Het bronsysteem toont haar eindgebruiker informatie over het wel of niet succesvol versturen van de notificatie.
- Het doelsysteem toont de informatie uit de notificatie aan de eindgebruiker. De eindgebruiker kan een dossier hierna opvragen (waarna een normale uitvraag volgt.)

Tonen Aanvragen

Notificatie dossier aanvragen

MOET ZWAAR HERSCHREVEN

Bronsystemen slaan binnenkomende 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-index van de aanvragende school (
- datum/tijdstip binnenkomst van aanvraag

Versturen Notificatie

Actor(s)	Goal(s)
Bronsysteem	Versturen Notificatie naar Doelsysteem.
Doelsysteem	Ontvangen Notificatie van Bronsysteem.

Basisvariant: Notificatie na ontvangst DocumentRequest

Na een eerder verzoek tot levering wordt na het klaarzetten van een Dossier een Notificatie verstuurd naar Doelsystemen die een verzoek tot levering hebben verstuurd. Voorafgaand wordt eerst een [[OSO:2017/Initiëren_notificatie]Noficatie Melding]] naar het Traffic Center gestuurd. Deze variant wordt hier verder uitgewerkt.

Basisvariant: Notificatie voor aanvraag bij SWV

Voor het initiëren van een uitwisseling tbv een aanvraag bij een SWV wordt een Notificatie met Koppelsleutel verstuurd naar het Doelsyteem. Voorafgaand wordt eerst een Notificatie Melding gestuurd. Deze variant wordt hier verder uitgewerkt.

Basisscenario

1. Bronsysteem verstuurt Notificatie naar Doelsysteem
2. Als Doelsysteem Notificatietype ondersteunt **AND** Doelsysteem kent Koppelsleutel
    1. Doelsysteem stuurt bevestiging ontvangst Notificatie aan BronSysteem*
    2. Doelsysteem toont Notificatie gegevens aan Eindgebruiker (Doelsysteem)**
    3. **IF** Bronsysteem heeft bevestiging ontvangen
        1. BronSysteem toont bevestiging aan Eindgebruiker (Bronsysteem)
    4. **ELSE**
        1. BronSysteem toont melding aan Eindgebruiker (Bronsysteem)***
    5. **ENDIF**
3. **ELSE**
    1. Doelsysteem stuurt foutcode naar Bronsysteem
    2. Bronsysteem toon foutmelding aan Eindgebruiker (Bronsysteem)
4. **ENDIF**

*Deze bevestiging is impliciet op basis van correct ontvangen van bericht
**Het doelsysteem toont de informatie uit de notificatie aan de eindgebruiker. De eindgebruiker kan een dossier opvraag sessie starten.
NB: De in de Notifciatie meegestuurde SessieID kan/mag NIET gebruikt worden voor het (opnieuw) opvragen van het dossier(!).
*** Het bronsysteem doet één poging per notificatie om deze te versturen na het doelsysteem; er volgen geen nieuwe pogingen wanneer de aflevering faalt. Het bronsysteem toont haar eindgebruiker informatie over het wel of niet succesvol versturen van de notificatie.

Uitzonderingen en meldingen

Resultaat	A/E*	Omschrijving	Toelichting
NotificatieOntvangen	Response door het Doelsysteem	De Notificatie wordt ontvangen door het Doelsysteem.	In het Doelsysteem wordt op basis van de ZoekSleutel in de Notificatie een Dossier opgevraagd bij het BronSysteem.
NotSupported		Het Doelsysteem ondersteunt dit type OSO uitwisseling niet.	Het Doelsysteem geeft aan dat een Notificatie van overdrachtsoort 'swv-aanvraag' is ontvangen, maar dat dit systeem deze functionaliteit niet ondersteund. Er vindt geen verdere verwerking plaats.
<Geen response>	E	Technische fout	Het meldende Bronsysteem staakt de verdere Notificatie en geeft de eindgebruiker hierover een foutmelding.

* A: Alternatief, E: Exceptie (fout)

Tonen Notificaties

Tonen ontvangen Notificaties

Doelsystemen slaan binnenkomende Notificaties op. Deze Notificaties moeten door eindgebruikers zichtbaar/opvraagbaar zijn.
De informatie over Notificatie(s) die getoond wordt moet voldoende zijn om een eindgebruiker in staat te stellen te beslissen om het dossier alsnog op te vragen. De minimale informatie die daarvoor getoond moet worden is:

- BSNleerling
- BRIN van de bronschool
- AP-index van het bron AP

De eingebruiker moet in staat zijn om in het Doelsysteem het desbetreffende Dossier aan te vragen.

Initiëren Terugkoppeling

Actor(s)	**Goal(s)**
Bronsysteem	Melden dat Bronsysteem Terugkoppeling aan Doelsysteem wil versturen en adres van Aanleverpunt ontvangen.
Traffic Center	Controleren of Terugkoppeling verstuurd kan worden en zorgen dat Terugkoppeling bij juist Aanleverpunt wordt afgeleverd.

NB: Bij deze beschrijving wordt Bronsysteem gebruikt als het SWV- of RP-systeem dat een Terugkoppeling wil versturen.

- Bronsysteem: Het SWV/RP systeem dat (voorafgaand aan deze uitwisseling) een Dossier heeft ontvangen

Dit betekent dat de richting van de Terugkoppeling wordt aangehouden en wordt afgeweken(!) van de richting van de Dossier uitwisseling .

Preconditie

- Bronsysteem is aangesloten op OSO keten
- Bronsysteem heeft Koppelsleutel ontvangen via Notificatie
- Bronsysteem heeft Dossier opgevraagd bij Doelsysteem met behulp van KoppelSleutel

Postconditie

- Traffic Center heeft Terugkoppeling Melding geregistreerd
- Bronsysteem heeft correcte url van Doelsysteem ontvangen

Basis scenario

1. Bronsysteem verstuurt Terugkoppeling Melding naar Traffic Center
2. **IF** DoelAanleverpunt is actief AND DoelAanleverpunt heeft 'doel' ingesteld op 'OV'
    1. **IF** KoppelSleutel valide is*
        1. Traffic Center registreert de Notificatie Melding
        2. Traffic Center geeft url van het Doelaanleverpunt terug
    2. **ELSE**
        1. Traffic Center geeft foutmelding
3. **ELSE**
    1. Traffic Center geeft foutmelding
4. **ENDIF**

***Valide Koppelsleutel** betekent dat de combinatie BronAP--KoppelSleutel--DoelAP is geregistreerd in het TC.

Uitzonderingen en meldingen

Hieronder worden alternatieve scenario's en de bijbehorende melding opgesomd:
.

Resultaat	**Omschrijving**	**Toelichting**	***Melding a Eindgebru***
<url van AP>	TC geeft url van (bron)AP (LAS) terug aan Doelsysteem (SWV/RP).	Bronsysteem (SWV/RP) kan nu Terugkoppeling versturen naar Bronsysteem (LAS).	Zie opmer boven ove gebruik do en bron-systeem.
AanvragerNietBekend	Het bronsysteem (aanleverpunt dat de notificatie meldt) is niet bekend bij het Traffic Center. De aanvrager is niet gerechtigd om de overstapservice te gebruiken.	In het Traffic Center register is de combinatie van bronBrin en bronAanleverpuntIndex niet aanwezig.	De aanvrag is niet gerechtigd de overstapse te gebruike Neem cont op met je leverancie
AanvragerAanleverpuntNietBekend	Het bronAanleverpuntIndex is niet geregistreerd voor deze aanvrager (bronBrin).		Het bron aanleverpu niet beken het OSO systeem, hierdoor k geen notifi melding worden aangevraag

Resultaat	**Omschrijving**	**Toelichting**	***Melding a Eindgebru***
AanvragerNietBeschikbaar	De aanvrager (bronBrin) is niet gerechtigd om de overstapservice te gebruiken.		Je school i niet aangeslote OSO. Nee contact op de service van OSO.
OngeautoriseerdAanleverpunt	Het OIN van het certificaat komt niet overeen met die van de geregistreerde leverancier. Het bronsysteem (aanleverpunt dat Notificatie meldt) is in het Traffic Center register geregistreerd door een andere leverancier.	Het aanleverpunt (bronBrin/bronAanleverpuntIndex) is bekend bij OSO, maar het aanleverpunt staat geregistreerd bij een andere leverancier.	Interne fou OSO syste Neem cont op met de servicedes van OSO.
VerstrekkerNietBekend	De verstrekker (het doelsysteem waar de notificatie naartoe verstuurd moet worden) is niet bekend bij het Traffic Center.		Het aanleverpu van de sch waarmee j wilt uitwissele nog niet bekend bij OSO. Nee contact op de betreffe school.
VerstrekkerAanleverpuntNietBekend	Het meegegeven aanleverpunt is niet geregistreerd voor deze verstrekker. Het opgegeven Aanleverpunt (DoelBRIN/APindex) van het Doelsysteem is niet bekend.	Het opgegeven Aanleverpunt van het Doelsysteem is (nog) niet opgenomen in het Register.	Het aanleverpu van de sch waarmee j wilt uitwissele nog niet bekend bij OSO. Nee contact op de betreffe school.
VerstrekkerNietBeschikbaar	De verstrekker is niet gerechtigd om de overstapservice te gebruiken. Het	De Doelschool is bekend in het Register, maar het opgegeven Aanleverpunt is (nog) niet actief. Dit kan bijvoorbeeld veroorzaakt	De school waarmee j wilt uitwissele

Resultaat	**Omschrijving**	**Toelichting**	***Melding a Eindgebru***
	opgegeven Aanleverpunt van het Doelsysteem is (nog) niet gerechtigd om de overstapservice te gebruiken.	worden doordat de URL van dit Aanleverpunt niet (goed) is geregistreerd	heeft geen actieve aanleverpu bij OSO. N contact op de betreffe school.
OnbekendeKoppelsleutel	De combinatie van KoppelSleutel-BronAP--KoppelSleutel-DoelAP is niet bekend bij het TC.	De KoppelSleutel geldt voor een specifieke Bronaanleverpunt-Doelaanleverpunt combinatie. Deze is niet gevonden in het TC register.	Er heeft zi een interne fout voorgedaa tijdens de SWV aanvraag. Neem cont op met je software leverancie
<Geen response>	Technische fout	Het meldende Bronsysteem staakt de verdere Notificatie en geeft de eindgebruiker hierover een foutmelding.	Er kan gee verbinding gemaakt worden me OSO syste Probeer he later nog e

Aanroep en antwoord

Element	Uitleg	Opmerkingen
bronBRIN	Dit is het brinnummer van de Bronschool waar de Terugkoppeling aan verstuurd wordt.	De Bronschool kan meerdere Aanleverpunten hebben.
bronAanleverpuntIndex	Dit is de index van het specifieke Aanleverpunt waar de Terugkoppeling aan verstuurd wordt.	Een Terugkoppeling wordt altijd naar één specifiek Aanleverpunt verstuurd.
doelBrin	Dit is het brinnummer van het Doelsysteem dat de Terugkoppeling aanmeldt. Het TC controleert of het Doelsysteem bekend en actief is in het deelnemersregister.	Zie opmerking boven over gebruik doel- en bron- systeem.
doelAanleverpuntIndex	Dit is de index van het Aanleverpunt van het Doelsysteem dat de Terugkoppeling aanmeldt.	Zie opmerking boven over gebruik doel- en bron- systeem.
koppelsleutel	De koppelsleutel zoals ontvangen in de Notificatie vanuit het Doelsysteem	De koppelsleutel is verplicht voor dit type uitwisseling

Versturen Terugkoppeling

Actor(s)	Goal(s)
Bronsysteem	Ontvangen Terugkoppeling van Doelsysteem.
Doelsysteem	Versturen Terugkoppeling naar Bronsysteem.

NB: Bij deze beschrijving wordt Bronsysteem gebruikt als het SWV- of RP-systeem dat een Terugkoppeling wil versturen.

- Bronsysteem: Het SWV/RP systeem dat (voorafgaand aan deze uitwisseling) een Dossier heeft ontvangen
- Doelsysteem: Het LAS dat de Terugkoppeling ontvangt (en voorafgaand aan deze uitwisseling een Dossier heeft verstuurd).

Dit betekent dat de richting van de Terugkoppeling wordt aangehouden en wordt afgeweken(!) van de richting van de Dossier uitwisseling .

Preconditie

- Bronsysteem is aangesloten op OSO keten
- Bronsysteem heeft TerugkoppelingMelding verstuurd naar Traffic Center
- Bronsysteem heeft Dossier opgevraagd bij Doelsysteem met behulp van KoppelSleutel
- Doelsysteem is aangesloten op OSO keten

Postconditie

- Doelsysteem heeft Terugkoppeling ontvangen van Bronsysteem

Basis scenario

1. Bronsysteem verstuurt Terugkoppeling naar Doelsysteem
2. Doelsysteem stuurt bevestiging ontvangst Terugkoppeling aan Doelsysteem*
3. Doelsysteem toont Terugkoppeling gegevens aan Eindgebruiker (Doelsysteem)**
4. **IF** Doelsysteem heeft bevestiging ontvangen
    1. Bronsysteem toont bevestiging aan Eindgebruiker (Bronsysteem)
5. **ELSE**
    1. Bronsysteem toont melding aan Eindgebruiker (Bronsysteem)***
6. **ENDIF**

*Deze bevestiging is impliciet op basis van correct ontvangen van bericht
**Het Doelsysteem toont de informatie uit de notificatie aan de eindgebruiker bij het desbetreffende Dossier. OSO vereist compleetheid van de informatie, maar stel geen verdere eisen aan de manier waarop een Doelsysteem dit inricht.
*** Het Bronsysteem doet één poging per Terugkoppeling om deze te versturen naar het Doelsysteem; er volgen geen nieuwe (automatische) pogingen wanneer de aflevering faalt. Het Bronsysteem toont haar eindgebruiker informatie over het wel of niet succesvol versturen van de Terugkoppeling. De eindgebruiker kan dan een nieuwe poging initiëren voor het versturen van een Terugkoppeling.

Uitzonderingen en meldingen

Hieronder worden alternatieve scenario's en de bijbehorende melding opgesomd:
.

Resultaat	**Omschrijving**	**Toelichting**	***Melding aan Eindgebruiker***
<Terugkoppeling>	De Terugkoppeling is succesvol ontvangen door het Doelsysteem.	Doelsysteem toont informatie van Terugkoppeling bij overeenkomstig Dossier.	Zie opmerking over gebruik bron- en doel-systeem boven.
KoppelSleutelOnbekend	Het Doelsysteem kent deze KoppelSleutel niet	Doelsysteem kan Terugkoppeling niet herleiden naar Dossier omdat Doelsysteem koppelsleutel niet kent en meldt dit aan het Bronsysteem.	Bronsysteem toont fout aan eindgebruiker.
NotSupported	Het Doelsysteem ondersteunt dit type OSO uitwisseling niet.	Het Doelsysteem geeft aan dat een Terugkoppeling is ontvangen, maar dat dit systeem deze functionaliteit niet ondersteund. Er vindt	De school waar de melding naar toe wordt verstuurd, heeft een systeem dat geen functie heeft voor het ontvangen van terugkoppelingen van dossiers. Neem

Resultaat	Omschrijving	Toelichting	*Melding aan Eindgebruiker*
		geen verdere verwerking plaats.	contact op met de betreffende school.
<Geen response>	Technische fout	Het meldende Bronsysteem staakt de verdere Terugkoppeling en geeft de eindgebruiker hierover een foutmelding.	Er kan geen verbinding gemaakt worden met het OSO systeem. Probeer het later nog eens.

Aanroep en antwoord

- Request:

Element	Uitleg	Opmerkingen
bronBRIN	Dit is het brinnummer van het Bronsysteem dat de Terugkoppeling verstuurt.	verplicht
bronAanleverpuntIndex	Dit is de index van het Aanleverpunt van het Bronsysteem dat de Terugkoppeling verstuurt.	verplicht
doelBrin	Dit is het BRINnummer van de Bronschool dat de Terugkoppeling ontvangt	verplicht
doelAanleverpuntIndex	Dit is de index van het Aanleverpunt van het Doelsysteem dat de Terugkoppeling ontvangt.	verplicht
KoppelSleutel	De KoppelSleutel die eerder is ontvangen door Bronsysteem van het Doelsysteem via een Notificatie met KoppelSleutel.	verplicht
Status	Informatie over de status van de Aanvraag (vrij tekstveld)	optioneel
Datum	Tijdstip waarop de Terugkoppeling werd verstuurd in het Bronsysteem.	verplicht
Bijlage(n)	Meegeleverde document(en). Hiervoor gelden dezelfde afspraken als die voor bijlagen bij een Dossier gelden (LINKX)	

- Response

Uitvoeren opvraag sessie

Context

Om een Dossier op te halen, start een Doelsysteem een Sessie. Hiervor vraagt een Doelsysteem een Sessie aan bij het Traffic Center. Het Traffic Center kent het Doelsysteem een Sessie toe als het Doelsysteem valide is én de Bronschool bekend is én valide Aanleverpunten heeft. Het Traffic Center geeft een lijst met Aanleverpunten door van de Bronschool. Na toekenning van een Sessie start het Doelsysteem met het bevragen van de Aanleverpunten van de Bronschool. Binnen de Sessie worden de Bronsystemen van een School in volgorde één voor één bevraagd [Aflopen aanleverpunten]. Na afloop wordt de Sessie afgesloten door het Doelsysteem bij het Traffic Center. In het afsluitverzoek wordt doorgegeven wat het *beste resultaat* van de Sessie was (Bijvoorbeeld: Dossier ontvangen, technische fout, etc.).

Preconditie

Doelsysteem is aangesloten op OSO en is valide.

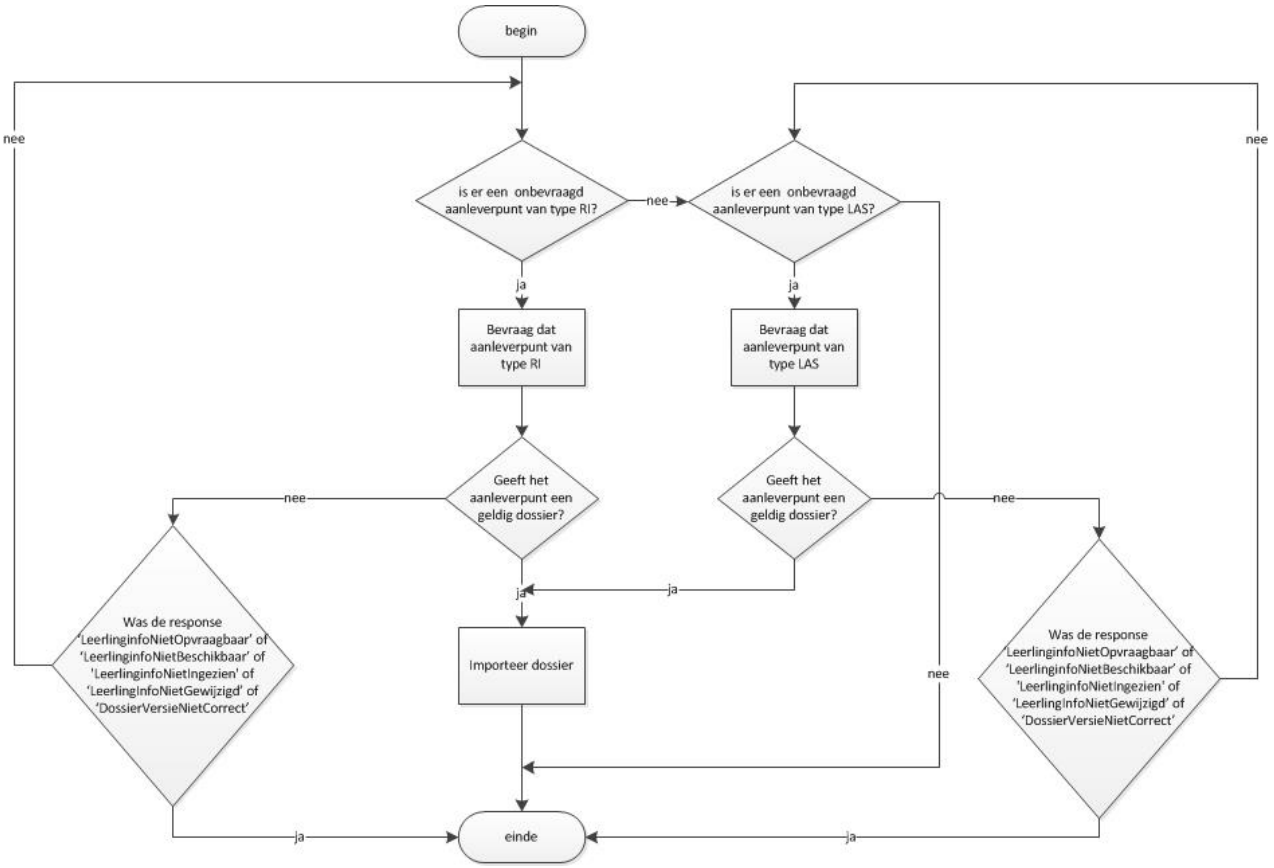
Postconditie

Sessie is afgesloten door Doelsysteem.

Basis Scenario

1. Systeem (doelschool) initieert sessie
2. **Zolang er** systemen (bronschool) van type ?RI? bij de doelschool niet bevraagd zijn:
    1. **Zolang er** geen dossier is ontvangen EN geen stopcriterium bereikt:
        1. Systeem (doelschool) vraagt specifiek dossier op bij eerstvolgend systeem (bronschool)
        2. **Als** systeem (doelschool) dossier heeft ontvangen:
            1. Systeem (doelschool) importeert dossier
3. **Zolang er** systemen (bronschool) van type ?LAS? bij de doelschool bij de doelschool niet bevraagd zijn is EN <geen stopcriterium bereikt>:
    1. **Zolang er** geen dossier is ontvangen of geen stopcriterium bereikt:
        1. Systeem (doelschool) vraagt specifiek dossier op bij eerstvolgend systeem (bronschool)
        2. **Als** systeem (doelschool) dossier heeft ontvangen:
            1. Systeem (doelschool) importeert dossier
4. Systeem (doelschool) meldt sessie af

Aflopen Aanleverpunten



Doorlopen sessie

Context

Om een Dossier op te halen, start een Doelsysteem een Sessie. Hiervor vraagt een Doelsysteem een Sessie aan bij het Traffic Center. Het Traffic Center kent het Doelsysteem een Sessie toe als het Doelsysteem valide is én de Bronschool bekend is én valide Aanleverpunten heeft. Het Traffic Center geeft een lijst met Aanleverpunten door van de Bronschool. Na toekenning van een Sessie start het Doelsysteem met het bevragen van de Aanleverpunten van de Bronschool. Binnen de Sessie worden de Bronsystemen van een School in volgorde één voor één bevraagd [Aflopen aanleverpunten]. Na afloop wordt de Sessie afgesloten door het Doelsysteem bij het Traffic Center. In het afsluitverzoek wordt doorgegeven wat het *beste resultaat* van de Sessie was (Bijvoorbeeld: Dossier ontvangen, technische fout, etc.).

Preconditie

Doelsysteem is aangesloten op OSO en is valide.

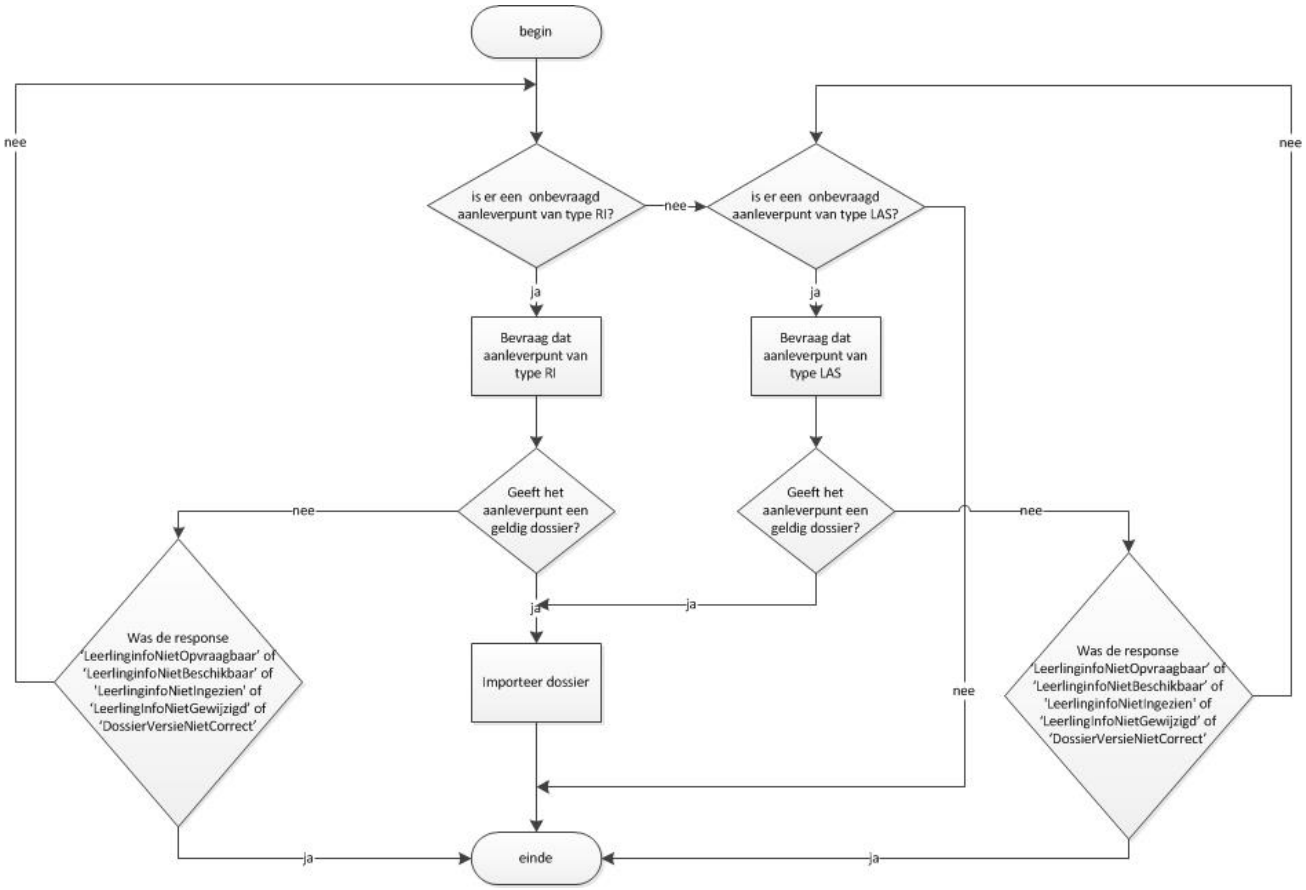
Postconditie

Sessie is afgesloten door Doelsysteem.

Basis Scenario

1. Systeem (doelschool) initieert sessie
2. **Zolang er** systemen (bronschool) van type ?RI? bij de doelschool niet bevraagd zijn:
    1. **Zolang er** geen dossier is ontvangen EN geen stopcriterium bereikt:
        1. Systeem (doelschool) vraagt specifiek dossier op bij eerstvolgend systeem (bronschool)
        2. **Als** systeem (doelschool) dossier heeft ontvangen:
            1. Systeem (doelschool) importeert dossier
3. **Zolang er** systemen (bronschool) van type ?LAS? bij de doelschool bij de doelschool niet bevraagd zijn is EN <geen stopcriterium bereikt>:
    1. **Zolang er** geen dossier is ontvangen of geen stopcriterium bereikt:
        1. Systeem (doelschool) vraagt specifiek dossier op bij eerstvolgend systeem (bronschool)
        2. **Als** systeem (doelschool) dossier heeft ontvangen:
            1. Systeem (doelschool) importeert dossier
4. Systeem (doelschool) meldt sessie af

Aflopen Aanleverpunten



Initiëren sessie

Actor(s)	Goal(s)
DoelSysteem	Geldige sessie toegekend krijgen voor opvragen specifiek dossier. Zowel in de variant met zoeksleutel als die met een koppelsleutel geldt dat een sessie altijd over één specifiek dossier gaat.
Traffic Center	Sessie toekennen aan systeem voor geldig verzoek van systeem voor specifiek dossier door school tbv overstap of aanvraag bij samenwerkingsverband

Basisvariant: Overstapdossier

Een Doelsysteem vraagt een Sessie aan om een specifiek Dossier op te vragen bij een School (BRIN(4)). Het TC verstrekt een Sessie wanneer de School bekend en actief is; er zijn actieve Aanleverpunten bij deze school die bevraagd kunnen worden. Het TC geeft de lijst met Aanleverpunten terug aan het Sessie aanvragende systeem. Het aanvragen van een Sessie voor deze variant wordt hier verder uitgewerkt.

Variant: Specifieke Aanleverpunt bevragen

Een Doelsysteem kan specifiek één Aanleverpunt bevragen door de APindex van dit Aanleverpunt mee te geven (samen met de BronBRIN). In dit geval geeft het TC geen lijst met Aanleverpunten terug, maar alleen de informatie van dit specifieke Aaneleverpunt (mits actief).

Basisvariant: Aanvraag bij Samenwerkingsverbanden

Een Doelsysteem vraag een Sessie aan na ontvangst van een Notificatie met een Koppelsleutel. De KoppelSleutel wordt gebruikt bij deze uitwisseling als aanduiding van het over te dragen Dossier. Het aanvragen van een Sessie voor deze variant wordt hier verder uitgewerkt.

Basis scenario

1. Doelsysteem vraagt Sessie aan bij TC
2. **IF** het Doelsysteem is valide[*] **AND** Doel Aanleverpunt is actief **AND** Bron School is actief **AND** (zoeksleutel **XOR** koppelsleutel is gevuld) **AND** (Overdrachtsoort correct ingevuld) **THEN**
    1. Traffic Center kent een sessie toe aan het Bronsysteem
    2. Traffic Center verstrekt lijst met te bevragen Aanleverpunten [**]
3. **Else**
    1. Traffic Center geeft foutcode terug
    2. Doelsysteem geeft foutmelding aan Eindgebruiker [***]

[*]Valide systeem houdt oa in dat het systeem gekwalificeerd is, een correct certificaat heeft en toegelaten is op de OSO keten.
[**]Als specifiek aanleverpunt bevraagd wordt, dan wordt alleen de gegevens van dit aanleverpunt doorgegeven door TC.
[***]In dit geval kan de Sessie niet afgemeld worden.

Uitzonderingen en meldingen

Hieronder worden alternatieve scenario's en de bijbehorende meldingen opgesomd:
.

Resultaat	**Omschrijving**	**Toelichting**	***Melding aan Eindgebruiker***
AanvragerNietBekend	De aanvrager (doelBrin) is niet gerechtigd om de overstapservice te gebruiken	Het doelBrin is niet bekend in het register van het Traffic Center.	Je school is niet aangesloten op OSO. Neem contact op met de servicedesk van OSO.
AanvragerAanleverpuntNietBekend	Het aanleverpunt van het doelsysteem (aanvragend aanleverpunt) is niet bekend bij het Traffic Center	In het Register is de combinatie van doelBrin en doelAanleverpuntIndex niet aanwezig.	Het aanleverpunt waarop je de leerling wilt ophalen is niet (goed) geregistreerd in je LAS.
AanvragerNietBeschikbaar	De aanvrager (doelBrin) is niet gerechtigd om de overstapservice te gebruiken.	De Doelschool (BRIN) is niet gerechtigd gebruik te maken van OSO.	Je school is niet aangesloten op OSO. Neem contact op met de servicedesk van OSO.
VerstrekkerNietBekend	Het bronBrin is niet bekend bij het Traffic Center.	De opgegeven bronschool is (nog) niet opgenomen in het	De school waar je de leerling ophaalt, is niet aangesloten op

Resultaat	**Omschrijving**	**Toelichting**	***Melding aan Eindgebruiker***
		Register van het Traffic Center.	OSO. Neem contact op met de betreffende school.
VerstrekkerAanleverpuntNietBekend	De bronBrin/APindex combinatie is niet bekend bij het Traffic Center.	Het opgegeven aanleverpunt van de bronschool is (nog) niet opgenomen in het Register van het Traffic Center.	De school waar je de leerling ophaalt, is niet aangesloten op OSO. Neem contact op met de betreffende school.
VerstrekkerNietBeschikbaar	Bronsysteem is niet gerechtigd om de overstapservice te gebruiken. Voorbeeld hiervan: de URL van het bronssysteem is niet (goed) geregistreerd.	De bronschool is bekend in het register, maar er zijn geen actieve aanleverpunten beschikbaar. Voorbeeld hiervan: de URL van het bronssysteem niet (goed) is geregistreerd.	De school waar je de leerling ophaalt, heeft geen actieve aanleverpunten bij OSO. Neem contact op met de betreffende school.
GeenRelatieMetDoel	De overdrachtSoort in het overdrachtsRequest is "overdrachtbinnenbrin" of “swv-aanvraag”, maar het bronBrin en doelBrin verschillen van elkaar.	Een overdracht binnenbrin mag alleen tussen systemen met eenzelfde BRIN plaats vinden.	Een overdracht "binnenbrin" mag alleen tussen systemen met eenzelfde BRIN-nummer plaatsvinden.
OverdrachtReedsActief	Er is reeds een sessie actief voor dezelfde parameters.	Een sessie voor een identieke overdracht is nog actief. Geldt *alleen* voor aanvraag met zoeksleutel.	Er is al een dossieroverdracht gestart. Probeer het over 10 minuten nog eens.
OVaanvraagMetKoppelsleutel	De aanvraag heeft een andere waarde voor overdrachtsoort dan 'SWVaanvraag' maar wel een Koppelsleutel ipv een Zoeksleutel ingevuld.	Een sessie wordt alleen toegekend bij een KoppelSleutel als de overdrachtsoort 'SWVaanvraag' is.	Er heeft zich een interne fout voorgedaan tijdens de SWV aanvraag. Neem contact op met je software leverancier.
OVaanvraagMetIncorrectAPtype	De aanvraag heeft een andere waarde voor overdrachtsoort dan	Een sessie wordt alleen toegekend bij een aanvraag met als	Er heeft zich een interne fout voorgedaan

Resultaat	Omschrijving	Toelichting	*Melding aan Eindgebruiker*
	'SWVaanvraag' maar het Doelaanleverpunt is van type 'SWV'	doelaanleverpunt van type 'SWV' als de overdrachtsoort 'SWVaanvraag' is.	tijdens de SWV aanvraag. Neem contact op met je software leverancier.
SWVaanvraagMetZoeksleutel	De aanvraag heeft overdrachtsoort 'SWVaanvraag' maar een Zoeksleutel ipv een KoppelSleutel ingevuld.	Een sessie voor een overdracht van overdrachtsoort 'SWVaanvraag' mag alleen een KoppelSleutel gebruiken.	Er heeft zich een interne fout voorgedaan tijdens de SWV aanvraag. Neem contact op met je software leverancier.
SWVaanvraagNietSpecifiek	De aanvraag van maakt gebruik van een zoeksleutel maar specificeert geen Bronanleverpunt.	Een sessie voor een overdracht van overdrachtsoort 'SWVaanvraag' moet een specifiek Bronaanleverpunt bevragen.	Er heeft zich een interne fout voorgedaan tijdens de SWV aanvraag. Neem contact op met je software leverancier.
SWVaanvraagMetIncorrectAPtype	De aanvraag heeft als waarde voor overdrachtsoort 'SWVaanvraag' maar het Doelaanleverpunt is van type 'LAS'	Een sessie wordt alleen toegekend bij een aanvraag met overdrachtsoort 'SWVaanvraag' als het doelaanleverpunt van type 'RP' of 'SWV' is.	Er heeft zich een interne fout voorgedaan tijdens de SWV aanvraag. Neem contact op met je software leverancier.
KoppelSleutelNietBekend	De aanvraag gebruikt een combinatie BronAP--Koppelsleutel--DoelAP die niet bekend is bij het TC.	Een koppelsleutel wordt door het TC gegenereerd bij het NotificatieRequest en moet daarom bekend zijn bij het TC.	Er heeft zich een interne fout voorgedaan tijdens de SWV aanvraag. Neem contact op met je software leverancier.
OngeautoriseerdAanleverpunt	Het OIN van het certificaat komt niet overeen met die van de geregistreerde leverancier	Het Aanleverpunt (BronBRIN/APindex) is bekend bij OSO, maar in het Register is een andere Leverancier bekend dat die deze sessie aanvraag indient.	Het aanleverpunt waarop je de leerling wilt ophalen is niet (goed) geregistreerd in je LAS.

Resultaat	Omschrijving	Toelichting	*Melding aan Eindgebruiker*
<Geen response>	Het Traffic Center geeft een time out of technische fout.	Het aanvragende Bronsysteem staakt de verdere aanvraag en geeft de eindgebruiker hierover een foutmelding.	Er kan geen verbinding gemaakt worden met het OSO systeem.

* A: Alternatief, E: Exceptie (fout)

overstap

Overstap variant

Actor(s)	Goal(s)
DoelSysteem	Geldige sessie toegekend krijgen voor opvragen specifiek dossier op basis van een zoeksleutel (Versleutelde PGN). Het betreft hier een LAS of een Regionaal Platform.
Traffic Center	Sessie toekennen aan systeem voor geldig verzoek van systeem voor specifiek dossier door school tbv overstap

Preconditie

Systeem (doelBrin) is toegelaten op OSO keten

- Doelsysteem heeft geldig *OSO certificaat*

Postconditie

Systeem heeft sessie toegekend gekregen voor opvragen specifiek dossier bij aangeduide systemen Systeem heeft lijst Aanleverpunten van doel 'OV' behorend bij bronBRIN ontvangen (Lijst kan leeg zijn.)

Aanroep en antwoord

- Request:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:ns="http://xml.eld.nl/schemas/Overstapservice/20170401">
   <soapenv:Header/>
   <soapenv:Body>
      <ns:overdrachtRequest>
         <ns:bronBrin>00YY</ns:bronBrin>


         <ns:doelBrin>12SS</ns:doelBrin>
         <ns:doelAanleverpuntIndex>1</ns:doelAanleverpuntIndex>

<ns:zoeksleutel>jlmNSPuT6wLmwzBXej/VktjYp2Too3CCNdcis5xzQaZKZYoJNzsimEwt+eH
UFI8TDi6hwVKvYX0EmoMRFHOOlyIjsC/36IZIUx7IFat5HU9WeUA+4MdDzQ/rbqD8jKPhhsAfl3
mmn/UwuBVdmoxu1BGLxUCioAu8+RhZ5DWW3Jc=</ns:zoeksleutel>
         <ns:overdrachtsoort>overstapdossier</ns:overdrachtsoort>
      </ns:overdrachtRequest>
   </soapenv:Body>
</soapenv:Envelope>
```

Element	Uitleg	Opmerkingen
bronBRIN	Dit is het brinnummer van de Bronschool waar dossier van specifieke leerling wordt opgevraagd.	De Bronschool kan meerdere Aanleverpunten hebben.
bronAanleverpuntIndex	Dit is de index van het Aanleverpunt van het Bronsysteem dat bevraagd wordt (optioneel).	Deze parameter wordt alleen meegegeven worden wanneer het doelsysteem één specifiek Aanleverpunt van de School wil bevragen. In plaats van alle Aanleverpunten af te lopen bij een Bronschool wordt alleen het gespecificeerde Aanleverpunt bevraagd. Dit biedt Doelsystemen een mogelijkheid voor het ondersteunen van (V)SO-scholen.
doelBrin	Dit is het brinnummer van het Doelsysteem dat de Sessie aanvraagt. Het TC controleert of het Doelsysteem bekend en actief is in het deelnemersregister.	
doelAanleverpuntIndex	Dit is de index van het Aanleverpunt van het Doelsysteem dat de Sessie aanvraagt.	
zoeksleutel	Het versleutelde pgn (bsn of onderwijsnummer) van de leerling van wie het dossier gaat worden opgevraagd.	De zoeksleutel is verplicht voor dit type uitwisseling
koppelsleutel	De koppelsleutel zoals ontvangen in de Notificatie vanuit het Bronsysteem	**De koppelsleutel mag niet voorkomen in dit type uitwisseling!**
overdrachtsoort	De overdrachtsoort moet voor alle berichten binnen de sessie gelijk zijn	Het brinnummer van het bron- 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/20170401">
         <over:overdracht>
            <over:aanleverpunt>
               <over:code>0</over:code>

<over:url>https://helpdesk.swp.nl/osoverstrekker.axd</over:url>
               <over:type>LAS</over:type>
               <over:label>00AH00000 LAS Het Stedelijk Lyceum locatie
Kottenpark</over:label>
            </over:aanleverpunt>
            <over:aanleverpunt>
               <over:code>7</over:code>

<over:url>https://hetstedelijk.swp.nl/osoverstrekker.axd</over:url>
               <over:type>LAS</over:type>
               <over:label>00AH07007 LAS</over:label>
            </over:aanleverpunt>
            <over:aanleverpunt>
               <over:code>8</over:code>

<over:url>https://hetstedelijk.swp.nl/osoverstrekker.axd</over:url>
               <over:type>LAS</over:type>
               <over:label>00AH08008 LAS</over:label>
            </over:aanleverpunt>
            <over:aanleverpunt>
               <over:code>9</over:code>

<over:url>https://hetstedelijk.swp.nl/osoverstrekker.axd</over:url>
               <over:type>LAS</over:type>
               <over:label>00AH09009 LAS</over:label>
            </over:aanleverpunt>
            <over:aanleverpunt>
               <over:code>11</over:code>

<over:url>https://hetstedelijk.swp.nl/osoverstrekker.axd</over:url>
               <over:type>LAS</over:type>
               <over:label>00AH11011 LAS</over:label>
            </over:aanleverpunt>
            <over:aanleverpunt>
               <over:code>17</over:code>

<over:url>https://hetstedelijk.swp.nl/osoverstrekker.axd</over:url>
               <over:type>LAS</over:type>
               <over:label>00AH17017 LAS</over:label>
            </over:aanleverpunt>
            <over:aanleverpunt>
               <over:code>18</over:code>

<over:url>https://hetstedelijk.swp.nl/osoverstrekker.axd</over:url>
               <over:type>LAS</over:type>
               <over:label>00AH00018 LAS Het Stedelijk Lyceum locatie
Kottenpark</over:label>
            </over:aanleverpunt>
```

```
            <over:sessieId>64fd2abc-bf28-4c2c-a084-
83a394232b19</over:sessieId>
         </over:overdracht>
      </over:overdrachtResponse>
   </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Variant: Specifieke Aanleverpunt bevragen

Een Doelsysteem kan specifiek één Aanleverpunt bevragen door de APindex van dit Aanleverpunt mee te geven (samen met de BronBRIN). In dit geval geeft het TC geen lijst met

Aanroep en antwoord

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:ns="http://xml.eld.nl/schemas/Overstapservice/20160411">
   <soapenv:Header/>
   <soapenv:Body>
      <ns:overdrachtRequest>
         <ns:bronBrin>00YY</ns:bronBrin>


         <ns:doelBrin>12SS</ns:doelBrin>
         <ns:doelAanleverpuntIndex>102</ns:doelAanleverpuntIndex>

<ns:zoeksleutel>yl/xKgjcxwvxryvCveYeefn3NzZY8xCyC3UIpR62S7nVMV51q8XJpgyucE
...
VtAEpVArQfJq644cxeL87GLlelkgMxNkL7nrxAZehsINL6mvvNPFskIbZzSgFUTDpI=</ns:zoe
ksleutel>
         <ns:overdrachtsoort>overstapdossier</ns:overdrachtsoort>
      </ns:overdrachtRequest>
   </soapenv:Body>
</soapenv:Envelope>
```

Element	Uitleg	Opmerkingen
bronBRIN	Dit is het brinnummer van de Bronschool waar dossier van specifieke leerling wordt opgevraagd.	De Bronschool kan meerdere Aanleverpunten hebben.
bronAanleverpuntIndex	Dit is de index van het Aanleverpunt van het Bronsysteem dat bevraagd wordt (optioneel).	Deze parameter wordt alleen meegegeven worden wanneer het doelsysteem één specifiek Aanleverpunt van de School wil bevragen. In plaats van alle Aanleverpunten af te lopen bij een Bronschool wordt alleen het gespecificeerde Aanleverpunt bevraagd. Dit biedt Doelsystemen een mogelijkheid voor het ondersteunen van (V)SO-scholen.
doelBrin	Dit is het brinnummer van het Doelsysteem dat de Sessie aanvraagt. Het TC controleert of het Doelsysteem bekend en	

Element	Uitleg	Opmerkingen
	actief is in het deelnemersregister.	
doelAanleverpuntIndex	Dit is de index van het Aanleverpunt van het Doelsysteem dat de Sessie aanvraagt.	
zoeksleutel	Het versleutelde pgn (bsn of onderwijsnummer) van de leerling van wie het dossier gaat worden opgevraagd.	
koppelsleutel	De koppelsleutel die door een bronsysteem aan het doelsysteem wordt doorgegeven via een Notificatie.	Als een koppelsleutel gebruikt wordt, vervangt deze de zoeksleutel (xor). Een sessie aanvraag kan niet met beide waarden tegelijk werken.
overdrachtsoort	De overdrachtsoort moet voor alle berichten binnen de sessie gelijk zijn	Het brinnummer van het bron- 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/20160411">
  <over:overdracht>
    <over:aanleverpunt>
      <over:code>0</over:code>
      <over:url>https://urlvandebronschoolap0.nl</over:url>
      <over:type>LAS</over:type>
      <over:label>00YY0000 Testschool OSO</over:label>
    </over:aanleverpunt>
    <over:aanleverpunt>
      <over:code>102</over:code>
      <over:url>https://urlvandebronschoolap102.nl</over:url>
      <over:type>LAS</over:type>
      <over:label>00YY0102 Testschool OSO</over:label>
    </over:aanleverpunt>
    <over:sessieId>08758bef-5f79-46e9-9e7f-64e842785c77</over:sessieId>
  </over:overdracht>
</over:overdrachtResponse>
</SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Aanleverpunten terug, maar alleen de informatie van dit specifieke Aanleverpunt (mits actief).

NB: type van teruggegeven AP is altijd van doel 'OV' én type 'LAS' of 'RP'

Opvragen dossier

Actor(s)	Goal(s)
Doelsysteem	Doelsysteem heeft dossier van specifieke leerling ontvangen
Bronsysteem	Verzoek tot overhandigen specifiek dossier afgehandeld

Basisvariant: Overdracht van Dossier

In deze variant wordt het Dossier aangeduid met de zoeksleutel. Deze variant wordt hier verder uitgewerkt.

Basisvariant: Aanvraag bij Samenwerkingsverbanden

In deze variant wordt het gevraagde Dossier niet aangeduid met de ZoekSleutel maar met de Koppelsleutel (die eerder door het TC is afgegeven). Deze variant wordt hier verder uitgewerkt.

Basisscenario

1. Doelsysteem vraag dossier op [#]
2. Bronsysteem laat Sessie Controleren bij TC[*]
3. **IF** Sessie valide
    1. **IF** (overdrachtsoort='overstapdossier') **OR** (overdrachtsoort == 'binnenBRIN'))[**]
        1. *Bronsysteem slaat aanvraag gegevens (PGN , sessie id, documentRequest, doel brin, doel AP index, aanvraagMoment) op ten behoeve van Notificatie*[**]
        2. **IF** dossier gereed is voor overdracht[***] **AND** Dossier aan Doelsysteem overgedragen mag worden[***] **AND** *verzameldatum van Dossier voldoet*[*****] **And** DossierVersie is correct
            1. Bronsysteem verstuurt dossier
        3. **ELSE**
        4. Bronsysteem verstuurt foutmelding[******]
        5. **ENDIF**
    2. **ELSEIF** (overdrachtsoort='SWVaanvraag')
    3. **IF** dossier gereed is voor overdracht[***] AND **DossierVersie is correct**
        1. Bronsysteem verstuurt dossier
    4. **ELSE**
        1. Bronsysteem verstuurt foutmelding
    5. **ENDIF**
4. **ELSE**
    1. Bronsysteem verstuurt foutmelding
5. **ENDIF**

[#] In OSO kan een Doelsysteem aangeven dat het alleen geínteresseerd is in een 'geactualiseerd' Dossier. Zie ook punt [****]

[*]**Dit is een verplichte stap**. Deze controle *moet voor* de andere controles worden uitgevoerd

door het Bronsysteem. Als de Sessie gegevens incorrect blijken, moet dit worden teruggegeven aan het Doelsysteem. Pas daarna volgen de andere stappen en controles.
** De 'normale' OSO verstap wordt in deze tak afgehandeld. De tweede tak is bedoelt voor de afhandeling van 'Passend Onderwijs' aanvragen.
***Het <LINK NAAR GEREEED ZETTEN>Dossier is klaargezet en (indien van toepassing) inzage heeft plaats gevonden
****Bij het Dossier is door de Eindgebruiker (Bronsysteem) <LINK NAAR GEREEDZETTEN>aangegeven dat het opgevraagd mag worden door de School (BRIN).

Variant: Opvragen met AanvraagDatum

****Als de optionele parameter in het documentRequest ?aanvraagdatum? door het Doelsysteem is ingevuld, vergelijkt het bronsysteem deze waarde met de verzameldatum van het Dossier:

- Als de ?aanvraagDatum? kleiner is dan de verzameldatum van het dossier ('na de vorige aanvraag is het dossier aangepast en ingezien'), volgt de ?normale? afhandeling van het request.
- Als de ?aanvraagDatum? groter of gelijk is dan de verzameldatum van het dossier ('na de vorige aanvraag is het dossier niet aangepast') geeft het bronsysteem de (nieuwe) melding ?LeerlingInfoNietGewijzigd? (als het dossier wel klaar staat voor het bronsysteem).
- NB: Deze parameter wordt **niet** toegepast bij uitwisselingen met de KoppelSleutel (zie hierboven).

Uitzonderingen en meldingen vanuit de Sessie controle

Mogelijk resultaat van de sessieControle bij het TrafficCenter	**Verstrekkingsfout (of dossier) die de bron in de documentResponse aan het doel teruggeeft**
<technische fout>	SessieOngeldig
SessieReedsAfgemeld	SessieReedsAfgemeld
SessieAfwijkend	SessieAfwijkend
SessieVerlopen	SessieVerlopen
SessieOngeldig	SessieOngeldig
VerstrekkerNietBekend	AuthenticatieVerstrekkerMislukt
VerstrekkerNietBeschikbaar	AuthenticatieVerstrekkerMislukt
VerstrekkerAanleverpuntNietBekend	AuthenticatieVerstrekkerMislukt
OngeautoriseerdAanleverpunt	SessieOngeldig
OnbekendAanleverpunt	SessieOngeldig
AanvragerNietBekend	SessieOngeldig
AanvragerAanleverpuntNietBekend	SessieOngeldig
AanvragerNietBeschikbaar	SessieOngeldig
GeenRelatieMetDoel	SessieOngeldig
Sessie is valide (zie hieronder)	*dossier* of LeerlingNietBekend of LeerlinginfoNietOpvraagbaar of LeerlinginfoNietBeschikbaar of LeveringGeweigerd of LeveringInBehandeling of LeerlinginfoNietIngezien of LeerlingInfoNietGewijzigd of DossierVersieNietCorrect

Uitzonderingen en meldingen

Hieronder volgt een overzicht van afwijkingen van de 'normale flow' zoals die door het bronsysteem gedetecteerd moeten worden een doorgegeven aan het doelsysteem. Voor de 'SWV-aanvragen' geldt dat de uitzonderingen 2, 4 en 5 **niet** van toepassing zijn.

- Uitzondering #2 'LeerlingInfoNietGewijzigd': De parameter 'datum gewijzigd' wordt genegeerd bij de SWV-aanvragen.
- Uitzonderingen #4 'LeerlinginfoNietOpvraagbaar' en #5 'LeerlinginfoNietIngezien' zijn niet van toepassing bij SWV-aanvragen omdat inzage niet nodig is.

'

Rangorde*	**Resultaat**	**Omschrijving**	**Stopcriterium bij aflopen aanleverpunten**	***Melding aan Eindgebruike***
0	<Document>	Het gevraagde document. *(Let op: In het afmeldingRequest moet dan status='VerstrekkingGeslaagd' worden gebruikt)*	ja	nvt
1	LeveringInBehandeling**	Het leverende systeem (bron) kan niet bepalen of het dossier al beschikbaar is of dat de leerling bij de bron bekend is. Het aanvragende systeem (doel) gaat verder met het opvragen van het dossier bij de andere aanleverpunten.	nee	nvt
2	LeerlingInfoNietGewijzigd	De inhoud van het Dossier is sinds de opgegeven 'aanvraagdatum? in het documentRequest niet gewijzigd.	ja	
3	DossierVersieNietCorrect	De versie van het dossier dat klaar staat wijkt af van de huidige versie (en kan daardoor niet correct geïmporteerd worden door het doelsysteem).	ja	De versies van het dossier tussen bron en doelsysteem wijken van elkaar af en kunnen niet verwerkt worden.
4	LeerlinginfoNietOpvraagbaar	Het Dossier mag niet worden verstrekt, omdat de ouders/leerling geen toestemming hebben verleend.	ja	Het dossier mag niet worden verstrekt, omdat de

Rangorde*	Resultaat	Omschrijving	Stopcriterium bij aflopen aanleverpunten	*Melding aan Eindgebruike*
				ouders/leerling geen toestemming hebben verleend.
5	LeerlinginfoNietIngezien	Het document mag (nog) niet worden verstrekt, omdat de ouders nog geen inzage hebben gehad.	ja	Het document mag (nog) niet worden verstrekt, omdat de ouders nog geen inzage hebben gehad in het dossier.
6	LeerlinginfoNietBeschikbaar	Het Dossier is (nog) niet klaargezet voor overdracht.	ja	Het dossier is (nog) niet klaargezet voor overdracht. Neem contact op met de betreffende school.
7	LeveringGeweigerd	Het verstrekkende bronsysteem had het dossier klaargezet voor een specifiek BRIN-nummer. Het verstrekkende bronsysteem heeft het dossier niet uitgeleverd aan het opvragende doelsysteem, omdat het BRIN van het opvragende doelsysteem niet overeenkomt met het BRIN waarvoor het dossier was klaargezet.	nee	Het dossier is niet klaargezet voor het BRIN-nummer van jouw school. Neem contact op met de betreffende school.
8	LeerlingNietBekend	De leerling met het opgegeven BSN of Koppelsleutel is niet bekend bij het leverende bronsysteem.	nee	Het BSN-nummer van de leerling is niet bekend bij de betreffende school. Controleer het BSN, of neem contact op met

Rangorde*	Resultaat	Omschrijving	Stopcriterium bij aflopen aanleverpunten	*Melding aan Eindgebruike*
				de betreffende school.
9	AuthenticatieVerstrekkerMislukt	Het leverende bronsysteem kon zich niet authenticeren bij het Traffic Center. Het opvragende doelsysteem hoeft hierop geen actie te ondernemen.	nee	De school waar het dossier wordt opgehaald, wordt niet herkend. Neem contact op met de betreffende school.
10	SessieAfwijkend	De overstapvraag wijkt af van die, waarmee de sessie verkregen is. Dit is het resultaat van de sessieControle.	nee	Er heeft zich een interne fout voorgedaan tijdens de overdracht. Neem contact op met je software leverancier.
11	SessieReedsAfgemeld	De sessie is al afgemeld en dus niet langer geldig. Dit is het resultaat van de sessieControle.	nee	Er heeft zich een interne fout voorgedaan tijdens de overdracht. Neem contact op met je software leverancier.
12	SessieVerlopen	De sessie is verlopen; de time-out is verstreken. Dit is het resultaat van de sessieControle.	nee	Er heeft zich een interne fout voorgedaan tijdens de overdracht. Neem contact op met je software leverancier.
13	SessieOngeldig	De sessie is ongeldig; bij het controleren van de Sessie gegevens door het Traffic Center is een fout	nee	Er heeft zich een interne fout voorgedaan

Rangorde*	Resultaat	Omschrijving	Stopcriterium bij aflopen aanleverpunten	*Melding aan Eindgebruike*
		geconstateerd. (Bijvoorbeeld: Het SessieID is nooit uitgedeeld, het SessieID was leeg, de aanvrager heeft geen geldige status). Deze foutcode moet doorgegeven worden wanneer andere foutmeldingen niet van toepassing zijn.		tijdens de overdracht. Neem contact op met je software leverancier.
14	OperatieNietOndersteund	Het bevraagde bronsysteem geeft aan geen Dossiers te kunnen leveren (Functie niet ingebouwd)	nee	De school waar het dossier wordt opgehaald, heeft een systeem dat geen functie heeft voor het versturen van dossiers. Neem contact op met de betreffende school.
15	Communicatiefout	Het leverende bronsysteem geeft geen antwoord of er treedt een (technische) fout op. Er is geen contact geweest met het leverende bronsysteem.	nee	Er treedt een (technische) fout op bij de school van herkomst.

* De rangorde geeft de 'mate van succes' van de overdracht aan, hoe hoger hoe beter. Bronsystemen moeten de 'laagste toestand' teruggeven aan het Doelsysteem; het Doelsysteem moet het 'hoogste resultaat' binnen één Sessie terugrapporteren bij het afsluiten van de Sessie.
**Deze melding is optioneel, niet alle systemen kennen deze toestand.

Controleren Sessie

Actor(s)	Goal(s)
Traffic Center	Bewaken van integriteit van sessie
Bronsysteem	Vaststellen dat ontvangen verzoek een valide en geldig verzoek voor een specifiek dossier is

Preconditie

- BronSysteem is toegelaten op OSO keten
- BronSysteem heeft geldig *OSO certificaat*
- BronSysteem heeft DossierRequest ontvangen van DoelSysteem

Postconditie

- Traffic Center heeft vastgesteld of gegevens uit verzoek voor Dossier overeenkomen met gegevens uit toegekende sessie.
- Traffic Center heeft vastgesteld dat Bron- én Doel- systeem valide en actieve systemen zijn binnen de OSO keten.

Basisvariant

1. **Als** Doelsysteem **en** Bronsysteem aangesloten zijn op OSO
    1. **Als** gegevens uit verzoek (Documentrequest) van Doelsysteem overeenkomen met gegevens uit sessie
        1. Traffic Center geeft sector van de Doelschool terug
        2. Bronsysteem levert Dossier aan Doelsysteem
2. **Anders**
    1. Traffic Center geeft foutmelding
    2. Bronsysteem geeft foutmelding door aan Doelsysteem

Uitzonderingen en 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/koppelsleutel moeten hetzelfde zijn als in het overdrachtsRequest.
OnbekendAanleverpunt	A	Het doelaanleverpunt (aanvragend AP) komt niet overeen met datgene wat in het overdrachtsRequest is gebruikt. Indien het bronaanleverpunt (verstrekkend AP) 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	Bronschool (BRIN) is niet bekend bij het Traffic Center
VerstrekkerAanleverpuntNietBekend	A	Bronaanleverpunt (BRIN + APindex) is niet bekend bij het Traffic Center
VerstrekkerNietBeschikbaar	A	Bronsysteem is niet gerechtigd om de overstapservice te gebruiken.
OngeautoriseerdAanleverpunt	E	Bronsysteem (aanvragend AP) is in het Register geregistreerd met andere Leverancier.
AanvragerNietBekend	A	De Doelschool (BRIN) is niet bekend bij het Traffic Center
AanvragerAanleverpuntNietBekend	A	Doelaanleverpunt (BRIN + APindex) is niet bekend bij het Traffic Center
AanvragerNietBeschikbaar	A	Doelsysteem (aanvragend AP) is (nog) niet gerechtigd om gebruik te maken van de overstapservice
SessieOngeldig	E	Het sessieId komt niet overeen met een door het TC uitgedeeld sessieID
SessieReedsAfgemeld	E	Het sessieId verwijst naar een sessie die al is afgemeld.
SessieVerlopen	E	Het sessieId is verlopen. Na 10 minuten verloopt de sessie.

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

Aanroep en antwoord

- Request (voorbeel van OV controle):

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:ns="http://xml.eld.nl/schemas/Overstapservice/20170401">
   <soapenv:Header/>
   <soapenv:Body>
      <ns:sessiecontroleRequest>
         <ns:bronBrin>00AH</ns:bronBrin>
         <ns:bronAanleverpuntIndex>18</ns:bronAanleverpuntIndex>
         <ns:doelBrin>12SS</ns:doelBrin>
         <ns:doelAanleverpuntIndex>1</ns:doelAanleverpuntIndex>


<ns:zoeksleutel>SytZo1IuJ+Q+efm0oSd5kRngAz6NgzGDgCQEt1jo/FmoFfNlandlJ+kyfET
aklBuoDPEVH0GVy5

ySuoWyNIFbLFXXKEk+0THR7swVYa2K33xspMbFaL00NM62mA/bjbhPUJdTcwdHk/OnxnWvu/fYy
5
 4y6Bn3hxkUf194biYk8=</ns:zoeksleutel>
         <ns:overdrachtsoort>swvaanvraag</ns:overdrachtsoort>
         <ns:sessieId>b8b9a132-51ca-4188-8de7-323842336156</ns:sessieId>
      </ns:sessiecontroleRequest>
   </soapenv:Body>
</soapenv:Envelope>
```

- Request (voorbeel van PaO controle):

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:ns="http://xml.eld.nl/schemas/Overstapservice/20170401">
   <soapenv:Header/>
   <soapenv:Body>
      <ns:sessiecontroleRequest>
         <ns:bronBrin>00AH</ns:bronBrin>
         <ns:bronAanleverpuntIndex>19</ns:bronAanleverpuntIndex>
         <ns:doelBrin>00AH</ns:doelBrin>
         <ns:doelAanleverpuntIndex>19</ns:doelAanleverpuntIndex>

         <ns:koppelsleutel>19677A96-B737-402E-B3B8-
24A3EEF32000</ns:koppelsleutel>
         <ns:overdrachtsoort>swvaanvraag</ns:overdrachtsoort>
         <ns:sessieId>60d2909f-169f-4cb0-8256-5d1d5af1491d</ns:sessieId>
      </ns:sessiecontroleRequest>
   </soapenv:Body>
</soapenv:Envelope>
```

Element	Uitleg	Opmerkingen
bronBRIN	Dit is het brinnummer van de bronschool die het het dossier moet uitleveren.	De bronschool kan meerdere aanleverpunten hebben.
bronAanleverpuntIndex	Dit is de index van het aanleverpunt van het bronsysteem dat bevraagd wordt (optioneel).	Deze parameter kan meegegeven worden als het doelsysteem één specifiek aanleverpunt van de school wil bevragen.
doelBrin	Dit is het brinnummer van het doelsysteem dat de sessie heeft aangevraagd met de overdrachtRequest. Het TC controleert of het doelsysteem bekend en actief is in het deelnemersregister.	
doelAanleverpuntIndex	Dit is de index van het aanleverpunt van het doelsysteem dat de sessie heeft aangevraagd met de overdrachtRequest.	
zoeksleutel	De zoeksleutel wordt overgenomen uit het documentRequest.	Afhankelijk van de overdrachtsoort zal of de zoeksleutel of de koppelsleutel gevuld (moeten) zijn.
koppelsleutel	De koppelsleutel wordt overgenomen uit het documentRequest.	Afhankelijk van de overdrachtsoort zal of de zoeksleutel of de koppelsleutel gevuld (moeten) zijn.
overdrachtsoort	De overdrachtsoort moet voor alle berichten in de sessie gelijk zijn	Het brinnummer van het bron- en doelBrin moet hetzelfde zijn voor een binnenbrin overdracht.
sessieId		

- 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/20170401">
         <over:sectorAanvrager>VO</over:sectorAanvrager>
      </over:sessiecontroleResponse>
   </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

aanvraag

Uitwisseling tbv aanvraag bij Samenwerkingsverband (SWV) variant

Actor(s)	Goal(s)
DoelSysteem (RP of SWV)	Geldige sessie toegekend krijgen voor opvragen specifiek dossier. Een sessie geldt altijd voor één specifiek dossier.
	Sessie toekennen aan systeem voor geldig verzoek van systeem voor specifiek dossier door school voor aanvraag bij samenwerkingsverband.
Traffic Center	Deze uitwisseling wordt gestart na ontvangst van een Notificatie met Koppelsleutel. De aanvraag wordt altijd gedaan bij het specifieke Aanleverpunt dat de Notificatie verzonden heeft.

Preconditie

- Doelsysteem is toegelaten op OSO keten
- Doelsysteem heeft geldig *OSO certificaat*
- Doelsysteem heeft Notificatie ontvangen van BronSysteem met KoppelSleuutel

Postconditie

- TC heeft DoelSysteem Sessie toegekend voor opvragen Dossier bij aangeduid Aanleverpunt van Bronsysteem.
- Doelsysteem heeft Aanleverpunt informatie met doel 'PaO' behorend bij bronBRIN ontvangen.

Aanroep en antwoord

- Request:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:ns="http://xml.eld.nl/schemas/Overstapservice/20170401">
   <soapenv:Header/>
   <soapenv:Body>
      <ns:overdrachtRequest>
         <ns:bronBrin>00AH</ns:bronBrin>


         <ns:doelBrin>00AH</ns:doelBrin>
         <ns:doelAanleverpuntIndex>19</ns:doelAanleverpuntIndex>
         <ns:koppelsleutel>19677A96-B737-402E-B3B8-
24A3EEF32000</ns:koppelsleutel>
         <ns:overdrachtsoort>swvaanvraag</ns:overdrachtsoort>
      </ns:overdrachtRequest>
   </soapenv:Body>
</soapenv:Envelope>
```

Element	Uitleg	Opmerkingen
bronBRIN	Dit is het brinnummer van de Bronschool waar dossier van specifieke leerling wordt opgevraagd.	De Bronschool kan meerdere Aanleverpunten hebben.
bronAanleverpuntIndex	Dit is de index van het Aanleverpunt van het Bronsysteem dat bevraagd wordt (optioneel).	Deze parameter wordt alleen meegegeven worden wanneer het doelsysteem één specifiek Aanleverpunt van de School wil bevragen. In plaats van alle Aanleverpunten af te lopen bij een Bronschool wordt alleen het gespecificeerde Aanleverpunt bevraagd. Dit biedt Doelsystemen een mogelijkheid voor het ondersteunen van (V)SO-scholen.
doelBrin	Dit is het brinnummer van het Doelsysteem dat de Sessie aanvraagt. Het TC controleert of het Doelsysteem bekend en actief is in het deelnemersregister.	
doelAanleverpuntIndex	Dit is de index van het Aanleverpunt van het Doelsysteem dat de Sessie aanvraagt.	
zoeksleutel	Het versleutelde pgn (bsn of onderwijsnummer) van de leerling van wie het dossier gaat worden opgevraagd.	**De zoeksleutel mag niet voorkomen in dit type uitwisseling!**
koppelsleutel	De koppelsleutel zoals ontvangen in de Notificatie vanuit het Bronsysteem	De koppelsleutel is verplicht voor dit type uitwisseling
overdrachtsoort	De overdrachtsoort moet voor dit type uitwisseling 'SWVaanvraag' zijn	Het brinnummer van het bron- 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/20170401">
         <over:overdracht>
            <over:aanleverpunt>
               <over:code>19</over:code>

<over:url>https://hetstedelijk.swp.nl/osoverstrekker.axd</over:url>
               <over:type>SWV</over:type>
               <over:label>00AH00019 SWV Het Stedelijk Lyceum locatie
Kottenpark</over:label>
            </over:aanleverpunt>
            <over:sessieId>cdf5c4d1-9cca-4116-9ed6-
ab575fc230a8</over:sessieId>
         </over:overdracht>
      </over:overdrachtResponse>
   </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

- **NB:** type van teruggegeven AP is altijd of 'RP' of 'SWV'

Opvragen met Koppelsleutel ipv Zoeksleutel

Een Doelsysteem kan specifiek een aanvraag starten na ontvangst van een Notificatie met Koppelsleutel. In dat geval wordt de sessie aangevraagd met deze Koppelsleutel en zonder(!) een Zoeksleutel. Een tweede eis is dat alleen het Aanleverpunt dat de notificatie heeft verstuurd naar het Doelsysteem bevraagd mag worden; er is sprake van een aanvraag bij een specifiek Aanleverpunt.

Importeren Dossier

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 gebruikersvriendelijkheid.

Tonen inhoud binnengekomen Dossier

Bij een import van een overstapdossier én een dossier conform ?Overdracht binnen brin? moet de applicatie alle binnengekomen gegevens, inclusief een lijst met de bijgesloten bijlagen (de metadata van de bijlagen), leesbaar tonen aan de geautoriseerde gebruiker d.m.v. een dossierweergave (bijv. een PDF). De dossierweergave is hiermee een compacte presentatie van alle gegevens en bijlagen die zijn overgedragen. Afhankelijk van de gegevensvelden, de gebruiker en het type applicatie kunnen leerlinggegevens in het overstapdossier na verwerking in de applicatie aan de gebruiker voor inzien (lezen) of wijzigen (schrijven) worden getoond. Bij een import van een dossier conform ?Overdracht binnen brin? is de applicatie vrij om gegevens te verwerken in de applicatie of te negeren.

De gegevens uit het Dossier moeten op een leesbare manier worden geformatteerd, gerangschikt en gepresenteerd. De codes uit de codetabellen moet vervangen door bijbehorende betekenisvolle ?labels?.

Uitwisseling voor aanvragen bij Samenwerkingsverband Passend Onderwijs

Bij het ophalen van Dossiers via deze overdrachtsoort (swv-aanvraag), wordt gebruik gemaakt van een eigen identificatie van het dossier, de koppelsleutel. Deze sleutel is uniek voor de combinatie van Bron Aanleverpunt - Dossier - Doel Aanleverpunt en wordt ook gebruikt bij de terugkoppeling. Een systeem dat een Dossier ontvangt via deze overdrachtsoort, **moet** de koppelsleutel bij het Dossier opslaan voor later gebruik.

Meervoudige ontvangst

Doelsystemen moeten om kunnen gaan met meerdere leveringen van hetzelfde dossier (identiek BSN) en deze correct kunnen afhandelen (Dossiers binnen gekomen via een overdracht van het soort 'swv-overdracht' worden éénmalig overgedragen en kennen **geen** meervoudige ontvangst!). Uitgangspunten hierbij zijn:

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

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 specificeren en voorschrijven tot de laatste stap en het kleinste detail veld. Leveranciers en scholen zullen hier zelf hun keuzen en uitwerkingen in moeten vinden.

Afmelden Sessie

Actor(s)	Goal(s)
Doelsysteem	Afronden opvraagsessie
Traffic Center	Afronden opvraagsessie en vastleggen resultaat van sessie

Context

Afmelden sessie is de laatste stap in het doorlopen van een transactie voor het opvragen van een dossier of het doorgeven van een notificatie.

- Dossier opvragen: Doelsysteem meldt sessie af bij Traffic Center en geeft 'beste resultaat': Het 'hoogste resultaat' op de resultaat tabel [reultaten] dat binnen de sessie teruggegeven is door een bevraagd Aanleverpunt.

Er kunnen meerdere aanleverpunten bevraagd zijn. Wanneer het beste resultaat bij meerdere aanleverpunten is behaald, dan moet het laatst bevraagde aanleverpunt met dat resultaat worden teruggegeven.

Preconditie

- Doelsysteem heeft een geldige sessie aangevraagd en toegekend gekregen
- Bronsysteem heeft een verzoek voor een specifiek dossier van Systeem (doelschool) ontvangen
- Bronsysteem heeft verzoek tegen sessie laten controleren door Traffic Center
- Bronsysteem heeft verzoek voor dossier afgehandeld
- Er zijn geen Bronsysteem meer beschikbaar die binnen deze sessie bevraagd kunnen worden.

Postconditie

1. Sessie is geregistreerd als afgerond door Traffic Center
2. 'Beste resultaat' is vastgelegd door Traffic Center

Basic Scenario

1. Doelsysteem verzoekt Traffic Center om sessie als afgerond te registreren
2. **IF** de sessie bekend is **AND** de sessie gegevens komen overeen met de gegevens in het verzoek
    1. Traffic Center registreert de sessie als afgerond
3. **ELSE** afwijking in sessie gegevens
    1. Traffic Center geeft foutmelding
    2. Doelsysteem beëindigt Sessie (geen terugkoppeling naar eindgebruiker)
4. **ENDIF**

Uitzonderingen en meldingen

Hieronder worden alternatieve scenario's en de bijbehorende melding opgesomd:
.

Resultaat	**Omschrijving**	**Toelichting**	***Melding aan Eindgebruiker***
OverdrachtGeslaagd	Afmelding is correct ontvangen door het Traffic Center	Afmelding is correct ontvangen door het Traffic Center en zal daar verder worden verwerkt.	NvT
AanvragerNietBekend	Doelsysteem is niet bekend bij het Traffic Center	In het Register is de combinatie van DoelBRIN en APindex niet aanwezig.	Je systeem probeert het document overdracht af te melden met een foutieve brin + aanleverpunt code combinatie.
AanvragerAanleverpuntNietBekend	Het meegegeven Aanleverpunt is niet geregistreerd voor deze aanvrager	Het Aanleverpunt is in het Register niet gekoppeld voor aan dit Doelsysteem/Leverancier	Het aanleverpunt waarmee de overdracht wordt afgemeld, is niet geregistreerd voor je school.
AanvragerNietBeschikbaar	Doelsysteem (aanvragend AP) is (nog) niet gerechtigd om gebruik te maken van de overstapservice	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.	Er heeft zich een interne fout voorgedaan tijdens de overdracht. Neem contact op met je software leverancier.
AanvragerNietGeautoriseerd	Doelsysteem (aanvragend AP) is in het Register	Het Aanleverpunt (BronBRIN/APindex) is bekend bij OSO, maar in het Register is een	Je systeem staat verkeerd geregistreerd in het OSO

Resultaat	**Omschrijving**	**Toelichting**	***Melding aan Eindgebruiker***
	geregistreerd met andere Leverancier.	andere Leverancier bekend dat die deze sessie aanvraag indient.	register, hierdoor kan de document overdracht niet afgemeld worden.
OnbekendAanleverpunt	Er is in 'SessiecontroleRequest' een aanleverpunt gebruikt, dat niet in de bijbehorende 'OverdrachtResponse' verkregen is.	Bij het initiëren van de Sessie geeft het TC een lijst met te bevragen Aanleverpunten terug. Dit meegestuurde Aanleverpunt was niet aanwezig in die lijst.	Er heeft zich een interne fout voorgedaan tijdens de overdracht. Neem contact op met je software leverancier.
VerstrekkerNietBekend	De verstrekker is niet bekend bij het Traffic Center	De gemelde Bronschool (BRIN) is niet geregistreerd.	Je systeem probeert de sessie af te melden met een BRIN van de bronschool dat niet bekend is in het OSO register.
VerstrekkerAanleverpuntNietBekend	Het meegegeven aanleverpunt is niet geregistreerd voor deze verstrekker	Het Aanleverpunt (BRIN + APindex) van de Bronschool is niet bekend in het Register.	Je systeem probeert de sessie af te melden met een meegegeven aanleverpunt dat niet is geregistreerd voor de verstrekker van het dossier.
VerstrekkerNietBeschikbaar	De verstrekker is niet gerechtigd om de overstapservice te gebruiken		Je systeem probeert de sessie af te melden met een Bronsysteem code dat niet gerechtigd om de

Resultaat	**Omschrijving**	**Toelichting**	***Melding aan Eindgebruiker***
			overstapservice te gebruiken.
SessieVerlopen	De sessie is verlopen; de sessie-time-out is verstreken.		De sessie kan niet worden afgemeld omdat deze reeds verlopen is.
SessieNietGecontroleerd	Bij de sessiecontrole is door het TC een sessiefout geconstateerd.	Het bevraagde Aanleverpunt kreeg deze fout terug bij het controleren van de Sessie	De sessie kon niet worden gecontroleerd en hierdoor niet worden afgemeld.
SessieOngeldig	De sessie is ongeldig; het ID is nooit uitgedeeld.	Het sessieId komt niet overeen met datgene wat verstrekt is in het overdrachtsResponse.	De sessie is ongeldig en kan hierdoor niet worden afgemeld.
SessieReedsAfgemeld	De sessie is al eerder afgemeld.		De sessie kan niet worden afgemeld omdat deze al afgemeld is.
OngeautoriseerdAanleverpunt	Bronsysteem (aanvragend AP) is in het Register geregistreerd met andere Leverancier.		Bronsysteem (aanvragend AP) is in het Register geregistreerd met andere Leverancier en hierdoor kan de sessie niet afgemeld worden.
<Geen response>	Het Traffic Center geeft een time out of technische fout.	Het aanvragende Bronsysteem staakt de verdere aanvraag en geeft de eindgebruiker hierover een foutmelding.	Het OSO systeem geeft een time out of technische fout en hierdoor kan de sessie niet afgemeld worden.

Aanroep en antwoord

- Request:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:ns="http://xml.eld.nl/schemas/Overstapservice/20170401">
   <soapenv:Header/>
   <soapenv:Body>
      <ns:afmeldingRequest>
         <ns:bronBrin>00AH</ns:bronBrin>
         <ns:bronAanleverpuntIndex>18</ns:bronAanleverpuntIndex>
         <ns:doelBrin>12SS</ns:doelBrin>
         <ns:doelAanleverpuntIndex>1</ns:doelAanleverpuntIndex>
         <ns:sessieId>b8b9a132-51ca-4188-8de7-323842336156</ns:sessieId>
         <ns:status>VerstrekkingGeslaagd</ns:status>
      </ns:afmeldingRequest>
   </soapenv:Body>
</soapenv:Envelope>
```

Element	Uitleg	Opmerkingen
bronBrin	Dit is het brinnummer van het Bronsysteem. Het TC controleert of het Bronsysteem bekend en actief is in het deelnemersregister. (Verplicht)	
bronAanleverpuntIndex	(Verplicht). Dit is het aanleverpuntnummer van het bronSysteem, dat (als laatste aanleverpunt) het overeenkomstige resultaat (uit de de documentResponse) heeft gegeven aan het doelSysteem.	Er kunnen meerdere aanleverpunten bevraagd zijn. Wanneer de beste resultaat bij meerdere aanleverpunten is behaald, dan moet het laatst bevraagde aanleverpunt met dat resultaat worden teruggegeven.
doelBrin	Dit is het brinnummer van het Doelsysteem. Het TC controleert of het Doelsysteem bekend en actief is in het deelnemersregister.	
doelAanleverpuntIndex	Dit is de index van het Aanleverpunt van het Doelsysteem.	
sessieId	Dit is de sessieId die ontvangen is in de overdrachtsResponse en gebruikt is in de communicatie met het bronSysteem.	
status	Dit is het resultaatbericht dat het doelsysteem heeft ontvangen bij het aflopen van de aanleverpunten bij het opvragen van een dossier in de documentRequest. Als het doelSysteem het dossier succesvol heeft ontvangen,	Bij meerdere meldingen van meerdere aanleverpunten wordt het 'beste resultaat' doorgegeven, bepaald door de hoogste plaats in

Element	Uitleg	Opmerkingen
	dan stuurt het bronSysteem geen foutmelding en moet het doelSysteem het resultaat 'VerstrekkingGeslaagd' meegegeven in het statusveld.	de tabel Meldingen bij opvragen Dossier.

- 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/20170401">
         <over:resultaat>SessieVerlopen</over:resultaat>
      </over:afmeldingResponse>
   </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

beveiliging

1. Uitgangspunten beveiliging: Waarom doen we dit?
2. Scope
3. Opzet beveiligingspagina's
4. Versleuteling BSN
5. Certificaten webservice adres
    - Leveranciers van certificaten
    - Geldigheidsduur (maximale termijn)
    - Type certificaat (domain, wildcard, SAN)
    - Sterkte en type sleutel
    - Wisselen sleutel
    - Ondertekeningsalgoritme
    - Type CSP validatie (DV, OV, EV)
    - Certificaat keten
6. Client certificaten
    - Leverancier van certificaten
    - Geldigheidsduur
    - Sterkte sleutel
    - Wisselen sleutel
    - Ondertekeningsalgoritme
    - Gebruik van het certificaat
    - Aanmelden van het certificaat
    - Implementatie client certificate authentication
7. Certificaat validatie
    - Verloopdatum
    - Intrekkingsstatus
    - Validatie certificaat keten
    - Certificaat voor de webservice geldig op het aangegeven domein?
    - Client certificaat geldig binnen de OSO keten?
8. Protocollen
    - HTTPS
    - HSTS
    - TLS
9. Informatiebeveiliging per interactie <UITBREIDEN MET NIEUWE INTERACTIES>
10. Controle procedure
11. Procedure bij (vermoeden van) misbruik
12. Geldigheid beveiligingseisen

uitgangspunten

Uitgangspunten voor de beveiliging van OSO

De beveiliging van OSO is gekoppeld aan overkoepelend beleid. Middels het beleid geven we aan wat we met OSO willen bereiken. Specifiek voor de beveiliging van OSO vinden we onderstaande standpunten het belangrijkst:

- We willen leerlingdossiers zo goed mogelijk beschermen tegen diefstal, misbruik en ongeoorloofde aanpassing
- We willen garanderen dat de overdracht van leerlingdossiers verloopt binnen alle door de wetgever gestelde eisen die gelden worden aan de omgang met persoonsgegevens
- We willen dat de overdracht van dossiers niet alleen veilig verloopt, maar ook voorziet in administratieve lastenverlichting binnen de OSO keten
- We willen de toegang tot data en systemen binnen de OSO keten alleen verlenen aan systemen die we vertrouwen
- We willen dat alle activiteiten binnen de OSO keten herleidbaar zijn tot een verantwoordelijke persoon

Deze standpunten vinden hun uitwerking in deze sectie van de wiki.

scope

Scope van de beveiligingsmaatregelen

Traffic Center

Het centrale component binnen OSO het Traffic Center. Hieronder vallen:

- De TC webservices
- De logging en verwerking daarvan, die gegenereerd wordt door het TC alsmede de aangesloten systemen in hun interactie met het TS

Aangesloten Systemen

Leerling Administratie Systemen (LAS), Samenwerkingsverbandsystemen (SWV) en Reginale Platforms (RP) die optreden binnen de OSO keten namens de scholen. Hieronder vallen:

- De webservices welke in contact staan met de OSO keten
- De verwerking van over te dragen en overgedragen leerlingsdossiers
- De logging van de interacties die een Systeem met het TC alsmede de andere op OSO aangesloten systemen heeft.

Eindgebruiker

De identificatie en het gedrag van eindgebruikers valt niet binnen de scope van de OSO beveiliging. Dit behoort expliciet toe aan de beveiligingsmaatregelen die worden opgelegd aan het LAS buiten OSO.

opzet paginas

De wiki pagina's onder OSO'16 zijn opgezet met een pagina per thema en per themapagina onderverdeeld in hoofdstukken per configuratie item. De items zijn onderverdeeld in **Eisen** met daaronder **Verklaring**.
De binnen de eisen genoemde bullets worden expliciet gemaakt door hier dik gedrukt te noemen:

- **moet**
- **mag niet**
- En varianten hierop

Hiermee wordt expliciet gemaakt dat aan deze eis, of onverwijld en volledig voldaan moet worden, of dat iets geen goed idee is, of dat iets niet gedaan mag worden. Het niet voldoen aan een eis vormt een blocker bij de kwalificatie.
Het is ook mogelijk dat de eis iets subtieler is:

- **onwenselijk**: Hetgeen genoemd is moet je eigenlijk niet willen en wordt afgeraden te doen. Het is echter (deze versie van OSO) geen blocker voor kwalificatie
- **acceptabel**: Hetgeen genoemd is voldoende sterk om veilig en betrouwbaar te gebruiken, echter zal dit niet een lange termijn oplossing zijn. Verbetering is wenselijk
- **zeer wenselijk**: Hetgeen genoemd is veilig en betrouwbaar, waardoor het ook op langere termijn blijft voldoen

De verklaring onder de eisen legt vervolgens uit hoe de eisen gelezen moeten worden, soms toegelicht met voorbeelden. Ook refereert de verklaring naar externe stukken waarin terug te lezen is waarom en bepaalde beveiligingseisen tot stand zijn gekomen.

versleuteling bsn

Versleuteling persoonsgebonden nummer (de zoeksleutel)

In het onderwijs wordt een persoonsgebonden nummer (PGN) gebruikt, meestal het BSN. In sommige gevallen hebben leerlingen (nog) geen BSN, bijvoorbeeld asielzoekers of leerlingen die niet in Nederland wonen. In dit geval krijgen ze een tijdelijk onderwijsnummer.

In dit stuk van de wet staat:

persoonsgebonden nummer (PGN):

het *burgerservicenummer (BSN)*, bedoeld in artikel 1, onder b, van de Wet algemene bepalingen burgerservicenummer, dan wel het door Onze Minister uitgegeven *onderwijsnummer*, bedoeld in artikel 27b, vierde lid

Een BSN moet voldoen aan een variant op de 11-proef. Het bsn kan op de volgende wijze gecontroleerd worden: (9*p1 + 8*p2 + 7*p3 + 6*p4 + 5*p5 + 4*p6 + 3*p7 + 2*p8 - p9) MOD11 = 0.

Een onderwijsnummer moet ook voldoen aan een variant op de 11-proef. Het onderwijsnummer kan op de volgende wijze gecontroleerd worden: (9*p1 + 8*p2 + 7*p3 + 6*p4 + 5*p5 + 4*p6 + 3*p7+ 2*p8) MOD11 = p9 + 5. Het onderwijsnummer begint altijd met een 1.

In de Overstapservice is het niet toegestaan om het PGN 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 versleuteling is gebaseerd op het RSA algoritme en er wordt dus gebruik gemaakt van een sleutelpaar. Er is een publieke sleutel welke bekend is bij elke leverancier en een privé sleutel welke alleen bekend is bij Kennisnet. Kennisnet kan de zoeksleutel ontsleutelen tot het PGN om te kunnen voldoen aan de zorgplicht (=> waar is een leerling heen gegaan?). Leveranciers kunnen de publieke sleutel verkrijgen bij OSO-support.

De zoeksleutel is de versleutelde combinatie van het prefix van 4 cijfers en het PGN van 9 cijfers.

typenummer/prefix	betekenis
2318	dit typenummergeeft aan dat het om een burgerservicenummer (BSN) gaat. Een voorbeeld van een BSN is 173999529. Het getal 2318173999529 moet versleuteld worden tot de zoeksleutel.
3872	dit typenummer geeft aan dat het om een tijdelijk onderwijsnummer gaat.

Een voorbeeld van een onderwijsnummer is 101211151. Het getal 3872101211151 moet versleuteld worden tot de zoeksleutel.

Voorbeeld: leerling heeft BSN 111222333, dan moet de combinatie 2318111222333 versleuteld worden tot zoeksleutel.

Hieronder volgt een voorbeeld van een (nep) RSA publieke sleutel.

```
 <RSAKeyValue>
 <Modulus>0EVKqqr5JyI4tYnOO1sDbazqyJY78rpBcvrcmbimjRkcwkpQ1knwVKURccH5
oaSdhaXptg+9QcBqbC0p3SLym7f3hyeLCJvxNEV4JPZ7L5GbnsC8Ux5HxLinW/B6mF8jM
Yh5du5X7OKytNA2qlGdwe7qM</Modulus>
 <Exponent>AQA2</Exponent>
 </RSAKeyValue>
```

De uitkomst van de versleuteling is de zoeksleutel. Deze sleutel wordt in het overdrachtsrequest meegestuurd. Bijvoorbeeld:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:ns="http://xml.eld.nl/schemas/Overstapservice/VERSIENUMMER">
  <soapenv:Header/>
  <soapenv:Body>
    <ns:overdrachtRequest>
      <ns:bronBrin>00YY</ns:bronBrin>
      <ns:bronAanleverpuntIndex>0</ns:bronAanleverpuntIndex>
      <ns:doelBrin>00YY</ns:doelBrin>
      <ns:doelAanleverpuntIndex>102</ns:doelAanleverpuntIndex>
      <ns:zoeksleutel>xz/Zn95R9aSdJ/BeNSQs231pogl9evDlUO8NIuAEKhfHWjV...dT4BA
7MkT3EBuYUEtPcRtBXY=</ns:zoeksleutel>
      <ns:overdrachtsoort>overdrachtbinnenbrin</ns:overdrachtsoort>
    </ns:overdrachtRequest>
  </soapenv:Body>
</soapenv:Envelope>
```

De zoeksleutel moet base64 encoded worden doorgegeven in het overdrachtsrequest en in het sessiecontrolerequest. In OSO moet hiervoor de 'standaard' Base64 content-transfer-encoding (zoals beschreven in RFC 4648, hoofdstuk 4), worden toegepast. NB: Deze encoding wijkt af van die toegepast in bijlagen(!).

Een bronsysteem moet ervoor zorgen dat de zoeksleutel zoals deze wordt ontvangen van het doelsysteem wordt doorgegeven aan het TC. Er mogen GEEN bewerkingen of conversies toe worden gepast op de inhoud op het formaat van de zoeksleutel om te voorkomen dat het TC de sessie onterecht ongeldig verklaard.

certificaten webservice

Leveranciers van certificaten

Certificaten worden uitgegeven door CA's (certificate authorities), via CSPs (Certificate Service Providers). De root CA's moeten vertrouwd worden door het systeem welke versleutelde verbindingen opzet. Om te bepalen welke CA's vertrouwd worden, gebruikt OSO een standaard lijst aan CA's. Deze lijst wordt beheerd door de Mozilla Foundation. Deze lijst wordt geregeld bijgewerkt en is direct online in te zien.
De CA's op deze lijst mogen certificaten uitgeven, dan wel een CSP middels delegatie certificaten laten uitgeven die gebruikt worden om de publieke webservices te beveiligen. Deze certificaten worden gekocht op domeinnaam door de SaaS leverancier.

Geldigheidsduur (maximale termijn)

Eisen

- Een certificaat voor de webservice mag **maximaal 3 jaar** geldig zijn

Verklaring

Certificaten zijn een technisch middel om te bewijzen welke identiteit een partij heeft en vormen de aanzet om te komen tot een versleutelde verbinding. Net als een echte ID kaart of paspoort, verlopen certificaten. Dit wordt gedaan om te voorkomen dat na verloop van tijd technisch kwalitatief ondermaatse certificaten in omloop blijven. Op het moment dat een certificaat niet langer betrouwbaar meer is, heeft deze automatisch voor een beveiligde keten geen toegevoegde waarde meer.
Gezien de elkaar snel opvolgende berichten betreffende de veiligheid van certificaten (denk aan de SHA1 hashing, onbetrouwbaar geworden CA's, etc.) is een maximale validiteit van 3 jaar gekozen. Hiermee wordt het Certificate Authority and Browser Forum (CA/B) gevolgd

Type certificaat

Eisen

- Een certificaat voor een enkel domein is **zeer wenselijk**
- Een SAN (Subject Alternative Name) certificaat is **acceptabel**
- Een Wildcard certificaat is **onwenselijk**

Verklaring

Een certificaat welke alleen geldig is voor een specifiek domein heeft maar een enkele plaats waar de privésleutel is opgeslagen, waardoor kans op diefstal beperkt of ongecontroleerde verspreiding is. Bij een SAN certificaat is de spreidingskans van de privésleutel al weer groter. In een SAN certificaat zijn expliciet de (sub)domeinen vastgelegd waarvoor het certificaat geldt. De privésleutel kan mogelijk op meerdere niet gerelateerde systemen actief zijn, waardoor kans op diefstal of onbeveiligde verspreiding groter is.

Een wildcard certificaat is onwenselijk, aangezien dit certificaat geldt voor alle subdomeinen onder het genoemde domein in het certificaat. Hierdoor is de spreidingsvlak van het certificaat oncontroleerbaar en loopt de privésleutel een aanzienlijk risico op diefstal of onveilige verspreiding. Het valt dan ook af te raden om wildcard certificaten in te zetten. Mocht dit wel noodzakelijk zijn voor de dienstverlening, dan moeten er binnen de organisatie duidelijke afspraken en technische maatregelen getroffen worden om de sleutel veilig te houden.

Sterkte en type sleutel

Eisen

- Een RSA sleutel **moet** minimaal 2048bit en maximaal 4096bit lengte zijn
- Mocht er gebruik gemaakt worden van elliptic curves als sleutel, dan moet dit minimaal een van volgende curves zijn:
    - secp256r1
    - secp384r1
    - secp521r1
- Een privésleutel **moet** veilig bewaard worden:
    - **Alleen leesbaar** door het proces dat de sleutel gebruikt (bijv. de webserver IIS of Apache)
    - **Niet gedupliceerd** naar andere systemen (CMDB, provisioning tools, templates, netwerkshares. etc)
    - Bij voorkeur beveiligd middels een wachtwoord

Verklaring

De sleutels die gebruikt worden voor zowel de publieke webservices (server certificaat) als wel de client certificaten welke gebruikt worden voor authenticatie van de client in de TLS sessie, moeten voldoen aan minimale sterkte eisen. De RSA privésleutel zal vrijwel overal gehanteerd worden. Hierbij is een sleutelsterkte van tenminste 2048bit noodzakelijk voor betrouwbare communicatie tussen partijen. Het verdient echter wel de aanbeveling om wanneer dit kan een sterkere sleutel te hanteren, bijvoorbeeld 3072bit of maximaal 4096bit. De reden dat er een maximum aan zit is omdat:

- Calculatie met grote sleutels een CPU intensieve operatie is, waarbij efficiency ten opzichte van het bereikte resultaat goed afgewogen moet zijn. 4096bit is met de huidige stand van de techniek zeker sterk genoeg en zal dat nog lang blijven
- Grote sleutels niet altijd ondersteund worden door software bibliotheken en TLS offloading hardware, waardoor compatibiliteitsproblemen kunnen ontstaan. Er moeten dan onevenredig grote investeringen gedaan worden om dit te corrigeren terwijl er op voorlopig geen toegevoegde waarde is

De veiligheid van de OSO keten valt of staat met de beveiliging van sleutels. Elke sleutel waarmee versleuteling, ondertekening, authenticatie, etc. wordt gedaan moet beveiligd zijn tegen ongeoorloofd gebruik. Dit geldt voor zowel externe gebruikers van het systeem als wel interne medewerkers zoals bijv. beheerders van het systeem.

Mogelijke oplossing

Onder Linux wordt een private sleutel bijvoorbeeld gegenereerd middels openssl. De veiligste keuze, genereert een RSA sleutel met 4096bit lengte en voorzien van een wachtwoord.

```
user@host $openssl genrsa -des3 -out private.pem 4096
```

Hetzelfde, maar dan zonder wachtwoord

```
user@host $openssl genrsa -out private.pem 4096
```

Het gebruik van een wachtwoord is veiliger maar omslachtiger. Elke keer als de webserver herstart en de sleutel laadt, moet het wachtwoord opnieuw ingevoerd worden. Uiteraard kan het proces automatisch gevoed worden met het wachtwoord, maar dan wordt alsnog ergens het wachtwoord opgeslagen. Mocht hiervoor gekozen worden, zorg dan in ieder geval dat het wachtwoord en de sleutel fysiek van elkaar gescheiden worden.

Wisselen sleutel

Eisen

- Als het certificaat vernieuwd wordt **moet** de privésleutel ook opnieuw gegenereerd worden

Verklaring

Een certificaat verloopt van nature omdat er zo een dwang ontstaat om een nieuw certificaat te genereren dat voldoet aan de dan weer geldende eisen van de techniek. Daarnaast zou dit ook moeten gelden voor privésleutels. De sleutelsterkte kan bijvoorbeeld sterker worden waardoor dit zinvol is. Daarnaast bestaat ook het risico dat de sleutel inmiddels te vaak getransporteerd is en het verstandig is de oude sleutel te vernietigen.

Ondertekeningsalgoritme

Eisen

- Ondertekening van certificaten **moet** gebeuren met tenminste SHA256

Verklaring

SHA1 wordt/is volledig in de ban gedaan omdat het onbetrouwbaar is als ondertekeningsalgoritme. De uitkomst van het algoritme is te voorspellen en dus onzichtbaar aan te passen, waardoor namaak ondertekeningen mogelijk zijn.

Type CSP validatie (DV, OV, EV)

Eisen

- Domain Validation is **onwenselijk**
- Organisation Validation **wenselijk**
- Extended Validation **zeer wenselijk**

Verklaring

Domein gevalideerde certificaten bieden weinig houvast betreffende de identiteit van een partij. Het certificaat wordt uitgegeven na het doorlopen van een volledig geautomatiseerd proces welke maar beperkte garantie geeft over de identiteit van de aanvrager. De enige controle die gedaan wordt is of de aanvrager iets met het domein kan doen (bijvoorbeeld mail ontvangen op het hostmaster mail adres). Dit is voor een vertrouwensketen onvoldoende en dus onwenselijk.

Organisatie gevalideerde certificaten geven wat meer informatie over de identiteit van een partij. Het certificaat bevat ten eerste daadwerkelijk identiteitsinformatie over de aanvragende partij. Daarnaast wordt uitgifte controle door de CA ook (deels) met de hand uitgevoerd. Er vindt bijvoorbeeld telefonische controle plaats of er worden (identiteits)papieren van de aanvrager vereist. De waarde van dit type certificaten is dan ook vele malen groter dan een domein gevalideerd certificaat en daarom op zijn minst wenselijk om te gebruiken.

Extended gevalideerde certificaten hebben de zwaarste vorm van validatie voordat ze worden uitgegeven, maar zeggen ook het meest over de houder van het certificaat. In een browser is zo'n certificaat ook te herkennen aan de groene balk in de adresbalk. Er vindt een intensieve controle plaats door de CA voordat een EV certificaat wordt uitgegeven. Hierbij dienen minimaal aanvullende bewijsstukken te worden opgeleverd over de identiteit van de aanvrager en de organisatie waarvoor deze werkt. Dit type certificaat zegt dan ook het meest over de betrouwbaarheid van het uitgegeven certificaat. In een beveiligde keten is dit type certificaat dan ook zeer wenselijk om te hanteren.

Certificaat keten

Eisen

- Er **moet** een certificaat keten met daarin alle intermediate certificaten worden meegeleverd door de webserver richting de client
- Er **moet** een certificaat keten met daarin alle intermediate certificaten worden meegeleverd door de client richting de webserver

Verklaring

Een certificaat keten bestaat uit het certificaat zelf, aangevuld met alle intermediate certificaten die worden meegeleverd door de CSP, de uitgevende instantie.
Het root certificaat moet niet meegeleverd worden, dat zit in de truststore van de andere partij.

Bij PKIoverheid bestaat de certificaat boom voor G2 certificaten bijvoorbeeld uit de issuers:
/C=NL/O=Staat der Nederlanden/CN=Staat der Nederlanden Root CA - G2 - **root, zit in de truststore**
|- /C=NL/O=Staat der Nederlanden/CN=Staat der Nederlanden Organisatie CA - G2 - **intermediate, moet worden meegestuurd**
|-- /C=NL/O=CSP Naam BV/OU=Issuing Certification Authority/CN=Naam CSP - PKI Overheid CA - G2 - **intermediate, moet worden meegestuurd**
|--- /C=NL/O=Uw organisatie/OU=Uw afdeling/CN=domein.tld/serialNumber=00000003KvKnummer0000 - **uw certificaat, moet worden meegestuurd**

Bovenstaande is indicatief. De werkelijke implementatie hangt af van de keuze voor een CSP en welke generatie certificaten er gekozen wordt (G2 of G3). Daarnaast is het mogelijk dat er nog een extra issuer certificaat in de boom aanwezig is. Ook deze issuer moet dan worden meegestuurd.

- De intermediate certificaten waar de server de ontvangen client certificaten tegen moet valideren zijn te downloaden op de site van PKIoverheid. De volgende intermediate certificaten moet worden gebruikt om client certificaten tegen te valideren:
    - G3
        - Stamcertificaat
        - Domein Organisatie Services
    - G2
        - Stamcertificaat
        - Domein Organisatie, maar alleen de volgende:
            - Staat der Nederlanden Organisatie
            - QuoVadis Trustlink
            - ESG CA
            - ESG Organisatie
            - KPN Corporate Market
            - KPN PKIoverheid Organisatie
            - Digidentity Organisatie **(Digidentity vereist nog een eigen intermediate certificaat, te downloaden bij Digidentity)**
- De intermediate certificaten die met het client certificaat moeten worden meegestuurd zijn te verkrijgen bij CSP waar het certificaat is gekocht.

client certificaten

Vanaf OSO'16 is overgegaan van certificaten per school naar certificaten per software leverancier, populair gezegd het "SaaS certificaat". Dit betekent dat voor elke koppeling naar een interface binnen OSO client authenticatie door het softwarepakket nodig is in plaats van authenticatie door de school. OSO geeft deze certificaten niet langer zelf uit maar heeft dit uitbesteed aan PKI Overheid. Een leverancier die actief is binnen OSO moet zichzelf voorzien van zo'n certificaat.
Validatie binnen OSO vindt plaats door te checken of:

- Het certificaat is uitgegeven door de correcte CA
- Het certificaat een OIN/HRN bevat dat gewhitelist is voor communicatie binnen de keten

De whitelist bevat alle OIN/HRNs van Leveranciers die gekwalificeerd zijn. In het Register wordt de lijst van aangesloten Leveranciers bijgehouden en hun relatie met Scholen (via de Aanleverpunten).

Leverancier van certificaten

Eisen

- Het client certificaat **moet** uitgegeven worden door een geaccrediteerd uitgever van "Staat der Nederlanden" certificaten.
- Het client certificaat **moet** ondertekend zijn door:
  - "Staat der Nederlanden Organisatie CA - G2" **of**
  - "Staat der Nederlanden Organisatie Services CA - G3"
- De service die de client certificaat validatie afdwingt **moet** exact alle 2 bovenstaande certificaat uitgevers accepteren
- De service die de client certificaat validatie afdwingt **moet** valideren dat de intermediate CA het client certificaat daadwerkelijk ondertekend heeft
- Het client certificaat **moet** een OIN/HRN bevatten, in het veld subject.serialNumber

Verklaring

Er zijn een aantal CSP's die namens de Staat der Nederlanden certificaten mogen uitgeven. Dit zijn commerciële partijen met elk hun eigen aanvraagprocedures en kosten. Het root CA blijft echter altijd "Staat der Nederlanden Root CA - G2" OF "Staat der Nederlanden Root CA - G3". Op moment van schrijven worden alleen nog certificaten uitgegeven vanuit de G2 root, het ligt echter in de lijn der verwachting dat dit op een gegeven moment overgaat naar de G3 root. OSO accepteert beide.
Binnen OSO wordt gebruik gemaakt van certificaten uit "Domein Organisatie Services" (G3) of "Domein Organisatie" (G2). Informatie over deze certificaten is na te lezen op de site van Logius.
OSO valideert de client certificaten alleen tegen bovengenoemde intermediate certificaten. Onder root CA Staat der Nederlanden worden nog meer typen certificaten uitgegeven dan de door OSO gebruikte service certificaten, bijvoorbeeld persoonscertificaten. Deze typen worden binnen OSO niet geaccepteerd, dus dat is dan ook de reden om niet tegen het root CA

certificaat te valideren, maar tegen een sub certificaat onder Staat der Nederlanden.
Op eerder genoemde site van Logius zijn de kenmerken van de certificaten in te zien en zijn de certificaten zelf ook te downloaden.

De gebruikte certificaten vallen onder de Digikoppeling standaard en zijn daarmee universeel inzetbaar voor communicatie met steeds meer overheidsdiensten. Meer informatie over de standaardisatie van deze certificaten is hier te lezen. Voor OSO is het OIN/HRN van belang. Lees met name vanaf pagina 23 door om te begrijpen hoe het OIN/HRN werkt.

Aanvullende informatie betreffende CSPs

Let op dat er een servercertificaat van PKIoverheid wordt gekozen. Hierbij moet je ervoor zorgen dat het OIN/HRN ingevuld is. Standaard wordt dit nummer op basis van het KvK-nummer gegenereerd, maar controleer dit goed. Zonder dit nummer is het certificaat voor OSO niet bruikbaar!!
Het standaard nummer is gebaseerd op het KVK nummer (00000003KvKnummer0000) en heet een HRN. Deze is alleen van toepassing voor bedrijven. Let op dat in geval van bedrijfsfusies, holdingen, etc, het juiste KvK-nummer wordt gebruikt!
Mocht de organisatie geen bedrijf zijn maar een overheidsgerelateerde organisatie, dan dient een OIN aangevraagd te worden. Alle OINs zijn in te zien in het register. Het spreekt voor zich dat het OIN bekend moet zijn alvorens het certificaat aangevraagd kan worden.

Lees voor aanvragen bij KPN ook de handleiding door.

Verklaring ten aanzien van DUO ODOC certificaten

Op het OSO technisch overleg van januari 2017 is besloten om de voor Edukoppeling 1.2 geldende DUO ODOC certificaten niet in te voeren voor OSO. Het is hierom alleen toegestaan om PKIoverheid certificaten te gebruiken voor client authenticatie.

Geldigheidsduur

Zie hiervoor de eisen bij de certificaten voor de webservice.

Sterkte sleutel

Zie hiervoor de eisen bij de certificaten voor de webservice.

Wisselen sleutel

Zie hiervoor de eisen bij de certificaten voor de webservice.

Ondertekeningsalgoritme

Zie hiervoor de eisen bij de certificaten voor de webservice.

Certificaat keten

Zie hiervoor de eisen bij de certificaten voor de webservice.

Gebruik van het certificaat

Het door PKI Overheid uitgegeven certificaat wordt alleen gebruikt op de Qualificatie- en Productie omgeving. Op de Sandbox omgeving worden certificaten gebruikt die nog wel door Kennisnet worden gegenereerd, maar verder geen enkele geldigheid op andere omgevingen of andere ketens vertegenwoordigen. Deze kunnen dan ook alleen ter test ingezet worden op Sandbox. Deze test certificaten kunnen worden aangevraagd via OSO support

Aanmelden van het certificaat

Het gekochte PKI Overheid certificaat moet bij Kennisnet worden aangemeld om zodoende het OIN/HRN te whitelisten op het Traffic-center. Dit kan door het certificaat aan te melden bij OSO Support. **Let op: lever ALLEEN het certificaat, niet een pfx, p12, private key of wat anders op. Alleen het publieke deel in de vorm van een crt of pem bestand.**

Implementatie Client Certificate Authentication

De OSO developers wiki beschrijft op een abstract niveau aan welke eisen systemen binnen de OSO keten moeten voldoen. In enkele gevallen is het echter toch gewenst een voorbeeld implementatie uit te werken. Dit geldt sterk voor de client certificate authenticatie op Windows systemen. Hierop is besloten voor IIS 8.5 een concrete uitwerking te maken. Deze is te lezen in de handreiking voor beheerders van Windows gebaseerde systemen: handleiding client authentication voor Windows.

certificaat validatie

Rijkwijdte

De genoemde validatie eisen hebben betrekking op alle voorkomende certificaten in de keten, te weten:

- Client certificaat
- Intermediate CA van het client certificaat, mits deze gebruikt wordt in de keten
- Root CA van het client certificaat
- Server certificaat
- Intermediate CA van het server certificaat
- Root CA van het server certificaat

Verloopdatum

Eisen

- Er **moet** gecontroleerd worden of de verloopdatum van geen enkel certificaat in de keten verlopen is
- Als een van de certificaten verlopen is, **moet** de verbinding direct verbroken worden

Verklaring

Certificaten hebben een vastgestelde geldigheidsperiode. Ze mogen niet voor en niet na de in het certificaat opgenomen periode gebruikt worden. Zie ook de eisen

Intrekkingsstatus

Eisen

- De intrekkingsstatus van een certificaat **moet** gecontroleerd worden
- Als een certificaat ingetrokken is **moet** direct de verbinding verbroken worden

Verklaring

Elke keer dat een certificaat geraadpleegd wordt moet gecontroleerd worden of de CA het niet heeft ingetrokken. Dit kan namelijk gebeuren omdat de partij van wie het certificaat is heeft besloten het terug te trekken omdat het een oud certificaat is dat is vervangen. Erger nog is als er iets mis is met deze partij dan wel de CA en dat de situatie niet meer te vertrouwen is, dan kan ook een certificaat worden teruggetrokken.
Ingetrokken certificaten mogen nooit gebruikt worden en zullen ook nooit meer in gebruik genomen worden. Er zal altijd een nieuw certificaat voor in de plaats moeten komen alvorens er weer gecommuniceerd mag worden met de partij van wie het certificaat was.

Validatie certificaat keten

Eisen

- Bij elke vorm van beveiligde communicatie **moet** altijd de gehele certificaat keten gecontroleerd worden op correct functioneren

Verklaring

De certificaat keten moet voordat gecommuniceerd wordt altijd worden gecontroleerd. Is het intermediate certificaat wel uitgegeven door een CA in de lokale truststore? Is het certificaat van de wederpartij wel uitgegeven door de door hen meegeleverde CA? Zie ook de eisen aan de server

Certificaat voor de webservice geldig op het aangegeven domein?

Eisen

- Het server certificaat dat uitgegeven is voor een specifiek domein **moet** overeenkomen met het domein in de URL. Er **mag geen** mismatch zijn tussen het domein waarvoor het certificaat bedoeld is en het domein dat opgevraagd wordt.
- De verbinding **moet** direct verbroken worden bij een domein mismatch.

Verklaring

Het server certificaat is uitgegeven met als doel een specifiek domein te beschermen. Als client is het dan ook de bedoeling alle afwijkingen hierop af te wijzen. Als het domein in het certificaat niet overeenkomt met het domein waar de verbinding mee wordt opgezet, dan moet de verbinding worden afgewezen. Mogelijk is er aan de serverkant van de wederpartij iets mis met de configuratie of in het slechtste geval de verbinding of gehele server gecompromitteerd.

Client certificaat geldig binnen de OSO keten?

Eisen

- Het client certificaat dat wordt ontvangen door de webserver wanneer een client zich wil authentiseren met zijn certificaat **moet** uitgegeven zijn door de CA of CA's die zijn geaccepteerd als certificaat leverancier binnen de OSO keten.
- De verbinding **moet** verbroken worden als het client certificaat niet van een geaccepteerde CA afkomstig is.

Verklaring

De client certificaten binnen OSO representeren een identiteit waarop vertrouwd moet kunnen worden. Deze identiteit wordt vastgesteld middels een vastomlijnde procedure, waar maar 1 of enkele CA's toe zijn gemachtigd om dit te doen. Op het moment dat een client certificaat is uitgegeven door een andere partij, ontstaat er geen vertrouwensrelatie tussen client en server. De server dient hierop de verbinding te verbreken.

client authentication windows

Om op Windows gehoste systemen client certificaat validatie toe te kunnen passen zijn soms behoorlijk wat stappen nodig. Deze zijn helaas niet even goed terug te vinden waardoor de implementatie nog wel eens op vraagtekens stuit. Er zijn verschillende mogelijkheden om dit voor elkaar te krijgen. Het kan binnen de applicatiecode worden opgelost, echter kan het ook volledig door IIS zelf gedaan worden. Om ondersteuning te bieden voor de laatste case is er een referentie handleiding geschreven. Deze handleiding werkt voor de 'kale' setup van IIS. Het spreekt voor zich dat dit geen uitputtende handleiding is, daarvoor zijn de mogelijke implementatiescenario's te divers.

Deze handleiding is geschreven voor Windows 2012r2 (Engelse editie) met IIS 8.5. Het zou ook moeten werken op Windows 2012 met IIS 8. Op eerdere versies van IIS werkt het niet, daar werkt client certificate authentication fundamenteel anders.

De handleiding gaat uit van een server met een al werkende webservice met een https endpoint en zonder gebruikmaking van ServerName Indication.

Eindresultaat van de handleiding is:

- De server accepteert alleen certificaten welke zijn uitgegeven onder de PKIoverheid Organisatie boom
- De server geeft de client de Acceptable Client Certificates lijst terug (TLS handshake veld 'certificate_authorities')

Register

Sta het verzenden van de Acceptable Client Certificates lijst toe middels een register aanpassing. Start regedit en pas de volgende sleutel aan / voeg deze toe:

```
DWORD
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHAN
NEL\SendTrustedIssuerList met waarde 1
```

Let op! Pas op voor spaties in de sleutel naam.

Accepteer alleen client certificaten als deze uitgegeven zijn door een vertrouwde leverancier (PKIoverheid). Hiervoor wordt een specifieke trustlist gehanteerd die in de komende hoofdstukken wordt geïmplementeerd. Hiervoor moet de standaard instelling onder Windows 2012 ingesteld staan. Als de volgende sleutel ingesteld is moet deze worden verwijderd of op waarde 0 worden ingesteld:

```
DWORD
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHAN
NEL\ClientAuthTrustMode
```

Issuer certificaten importeren

- Download de Organisatie certificaten van https://cert.pkioverheid.nl/. (Zoals uitgelegd verderop op de wiki)
- Het is belangrijk om de certificaten te importeren naar de Local Machine in de import wizard
- Selecteer in de import wizard een custom Certificate store: Client Authentication Issuers
- Importeer de twee PKIoverheid Organisatie issuer certificaten van PKIoverheid naar deze certificate store: Staat der Nederlanden Organisatie CA - G2 en Staat der Nederlanden Services CA - G3

IIS configuratie

- Open de IIS Manager en selecteer de website waar je de client certificate authentication aan wil toevoegen
- Er wordt van uitgegaan dat er op deze website al een https binding actief is. Check voor de zekerheid dat is inderdaad het geval is alvorens je verder gaat
- Open in IIS de websites SSL Settings en zet daar Require SSL aan en selecteer Require onder Client certificates. Pas de changes vervolgens toe
- Start een nieuwe shell en typ:

```
netsh
http
show sslcert
```

Kopieer de Certificate Hash, Application ID en Certificate Store Name waarden. Deze zijn later weer nodig. Typ nu:

```
delete sslcert ipport=0.0.0.0:443
```

Let bij het volgende commando op de quotes!!

```
add sslcert ipport=0.0.0.0:443 certhash=<your hash> appid="<your app id>"
sslctlstorename=ClientAuthIssuer certstorename=<your cert store>
clientcertnegotiation=enable
show sslcert
```

Dit zou moeten resulteren in de volgende uitvoer:

```
IP:port                      : 0.0.0.0:443
Certificate Hash             : <your hash>
Application ID               : <your id>
Certificate Store Name       : <your cert store>
Verify Client Certificate Revocation : Enabled
Verify Revocation Using Cached Client Certificate Only : Disabled
Usage Check                  : Enabled
Revocation Freshness Time    : 0
URL Retrieval Timeout        : 0
Ctl Identifier               : (null)
Ctl Store Name               : ClientAuthIssuer
DS Mapper Usage              : Disabled
Negotiate Client Certificate : Enabled
```

Testen

Het resultaat van alle changes is te zien met de volgende commando's.

```
openssl s_client -connect <domain of your service>:443
```

Naast andere uitvoer, moet je in ieder geval terug zien komen:

```
Acceptable client certificate CA names
/C=NL/O=Staat der Nederlanden/CN=Staat der Nederlanden Organisatie Services
CA - G3
/C=NL/O=Staat der Nederlanden/CN=Staat der Nederlanden Organisatie CA - G2
```

Op de server zelf kan je testen met een verzoek naar localhost in de browser (https://localhost). Het volgende zou teruggegeven moeten worden (na het accepteren van een certificaat waarschuwing omdat het server certificaat niet geldt voor localhost): HTTP Error 403.7 - Forbidden

Met een tool als cURL kan je checken of de client certificaat acceptatie werkt zoals verwacht:

```
curl -k -E /path/to/full/cert_bundle.pem https://<domain of your service>
```

De webpagina of de uitkomst van de webservice moet nu zijn zoals je die ook zou verwachten voordat je client certificaat authentication had aangezet. Als je nu hetzelfde request doet met een client certificaat van een niet door OSO geaccepteerde issuer of helemaal zonder client certificaat, dan moet je http error 403 (Access is denied) zien.

Als het nu niet werkt, dan is het belangrijk om te weten dat client certificate authentication internet toegang vereist voor de server. Het authentication proces in IIS vereist namelijk het downloaden van de issuers CRL (certificate revocation list). Wanneer je HTTP status 403 (substatus 13) in de IIS logs ziet voor elk request (met of zonder certificaat) dan kan de CRL niet gedownload worden. In dit geval moet je een uitgaande connectie toestaan in de firewall, of je moet een outbound http proxy instellen op de server.

Proxy

Als je een proxy gebruikt, moet je IIS instellen zodat deze de proxy ook gebruikt:

- Als dit nog niet zo is, zet de proxy settings in Internet Explorer op de server
- Hergebruik de netsh shell en typ de volgende regels:

```
winhttp
```

- Check of er niet toch een proxy is ingesteld. Zo ja, check of dit wel correct en delete anders deze settings

```
show proxy
import proxy source=ie
```

- Check of de nieuwe settings er in staan

```
show proxy
```

- Probeer de certificate tests opnieuw

Issues

Mocht je nog steeds tegen issues aanlopen, check dan grondig de ingevulde waarden. Volg ook de volgorde van de opgegeven commando's zodat alle configuratie correct aan elkaar gelinkt is. Probeer in het uiterste geval een reboot van IIS en anders de gehele server.

NB. Verander nu niet meer de https bindings in de IIS GUI. Doe je dit wel dan verwijder je ook alle settings die je met netsh hebt gemaakt voor deze binding.

protocollen

HTTPS

Eisen

- Er **moet** gebruik gemaakt worden van HTTPS
- Er **moet** gebruik gemaakt worden van een Fully Qualified Domain Name
- Er **moet** gebruik gemaakt worden van TCP port 443
- Er **mag geen** gebruik gemaakt worden van redirects die vanaf http (port 80) redirecten naar https (port 443).

Verklaring

De verbindingen binnen de OSO keten moeten van A tot Z beveiligd verlopen, hiervoor wordt HTTPS gebruikt. Om betrouwbaar te communiceren met partijen hebben deze een server certificaat nodig welke deze in de markt aanschaffen. Dit certificaat bevat de, of meerdere, domeinnaam of -namen. De betrouwbaarheid wordt vergroot door alleen gebruik te maken van volledige en traceerbare domeinnamen, Fully Qualified Domain Names (FQDN). HTTPS is door het IANA gestandaardiseerd op port 443, waar bij OSO dan ook gebruik van wordt gemaakt. Hiervan mag om compatibiliteitsredenen niet afgeweken worden.
Er mag geen redirect beschikbaar zijn welke de webservice calls redirect vanaf port 80 naar port 443. Als er op dezelfde host zowel http als https beschikbaar is, moet er een foutmelding teruggegeven worden als er OSO webservice calls op http binnenkomen.

```
400 Bad Request
Plain text http not supported, use https.
```

De reden hiervoor is dat een call over http direct al payload bevat waar datalekken risicovol kunnen zijn. Om te voorkomen dat verkeerd geconfigureerde clients toch kunnen doorgaan met het gebruik maken van deze onveilige redirect functie, mag er helemaal geen redirect gedaan worden. De client is hierdoor gedwongen zijn configuratie aan te passen.

HSTS

Eisen

- Het gebruik van de HSTS HTTP header is **niet verplicht**
- De maatregelen die door HSTS worden voorgeschreven, worden binnen OSO expliciet vereist in andere delen van het PvE

Verklaring

HSTS wordt alleen gebruikt door webbrowsers, waardoor verplichte implementatie en validatie niet het gewenste effect zal opleveren. Echter, de meeste eisen die HSTS oplegt worden al door het PvE afgedekt.

TLS

Versie

Eisen

- **Alleen** TLS versie 1.2 mag worden toegestaan
- Aan deze eis **moet** aan zowel de vragende (client) als wel de leverende (server) kant binnen OSO voldaan worden

Verklaring

TLSv1.2 is het beste protocol beschikbaar om communicatie tussen publieke http based webservices te beveiligen. SSLv2 en SSLv3 zijn al langere tijd niet meer veilig, echter zal dit ook niet lang meer duren voor TLSv1.
De belangrijkste voordelen van TLSv1.2 boven TLSv1.1 zijn dat er in v1.2 een flink aantal verbeteringen zijn doorgevoerd in de hashing functies, de requirements binnen het protocol een stuk strakker zijn gemaakt en er een aantal sterke AES gebaseerde ciphers bij zijn gekomen die meteen gebruikt worden binnen OSO.
Zowel de client als server moeten aan dezelfde TLS specificaties voldoen om te voorkomen dat een Man in the Middle aanval kan slagen door gebruik te maken van zwaktes aan een van beider zijden.

Mogelijke oplossing

Serverside

- De webserver staat in de configuratie van de webserver (bijvoorbeeld IIS of Apache) bij TLS alleen TLSv1.2 toe, waardoor clients andere versies nooit een verbinding kunnen opzetten
- De webserver filtert de TLS versie op de applicatielaag en staat voor de OSO webservices alleen TLSv1.2 toe. Deze optie is de workaround en verdient niet de voorkeur.

De 'workaround variant' heeft wat uitleg nodig.
Een bronsysteem controleert bij een binnenkomende aanvraag (documentRequest), voordat de aanvraag wordt afgehandeld, op welk TLS-niveau wordt gecommuniceerd. Wanneer dit niet TLSv1.2 is (maar bijv. TLSv1 of TLSv1.1) dan mag er geen dossier worden uitgeleverd(!). In plaats daarvan moet er een HTTP 400 fout worden terug gegeven en de volgende SOAP envelop:

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <soap:Fault>
      <faultcode>soap:Server</faultcode>
      <faultstring>TLS version not supported, use 'TLSv1.2'</faultstring>
    </soap:Fault>
  </soap:Body>
</soap:Envelope>
```

Dit geeft de aanvragende partij voldoende informatie over het mislukken van de aanvraag om maatregelen te treffen en deze af te vangen voor de eindgebruiker.

Ciphersuites en PFS

Eisen

Verplichte lijst: De volgende ciphersuites **moeten** ondersteund worden:

1. 0x2F ECDHE-RSA-AES128-GCM-SHA256
2. 0x30 ECDHE-RSA-AES256-GCM-SHA384
3. 0x27 ECDHE-RSA-AES128-SHA256
4. 0x28 ECDHE-RSA-AES256-SHA384

Keuze lijst: De volgende ciphersuites **mogen** ondersteund worden:

1. 0x2B ECDHE-ECDSA-AES128-GCM-SHA256
2. 0x2C ECDHE-ECDSA-AES256-GCM-SHA384
3. 0x13 ECDHE-RSA-CHACHA20-POLY1305
4. 0x2B ECDHE-ECDSA-CHACHA20-POLY1305
5. 0x23 ECDHE-ECDSA-AES128-SHA256
6. 0x24 ECDHE-ECDSA-AES128-SHA256

Keuze lijst: De volgende ciphersuites **mogen** ondersteund worden, maar wel met een opmerking:

1. 0x9E DHE-RSA-AES128-GCM-SHA256
2. 0x67 DHE-RSA-AES128-SHA256
3. 0x6B DHE-RSA-AES256-SHA256

Opmerkingen bij DHE:

- **Vereist** zelf gegenereerde DH parameters
- **Vereist** DH sleutel lengte van tenminste 2048bit (gelijk aan RSA privé sleutel)
- Lange DH sleutels genereren een behoorlijke performance hit op de systemen die ze gebruiken. Wanneer sterke versleuteling vereist is zou ECDHE ingezet moeten worden. ECDHE is vele malen lichter in gebruik.

Als alle bovenstaande ciphersuites worden toegepast **moet** onderstaande volgorde worden aangehouden:

1. ECDHE-RSA-AES128-GCM-SHA256
2. ECDHE-ECDSA-AES128-GCM-SHA256
3. ECDHE-RSA-CHACHA20-POLY1305
4. ECDHE-ECDSA-CHACHA20-POLY1305
5. ECDHE-RSA-AES256-GCM-SHA384

6. ECDHE-ECDSA-AES256-GCM-SHA384
7. ECDHE-RSA-AES128-SHA256
8. ECDHE-ECDSA-AES128-SHA256
9. ECDHE-RSA-AES256-SHA384
10. ECDHE-ECDSA-AES256-SHA384
11. ECDHE-ECDSA-AES256-SHA
12. DHE-RSA-AES128-GCM-SHA256
13. DHE-RSA-AES128-SHA256
14. DHE-RSA-AES256-SHA256

Mochten bepaalde ciphers uit de niet-verplichte lijsten niet gehanteerd worden, dan deze uit deze lijst verwijderen.
Ciphersuites welke niet genoemd zijn **mogen niet** gebruikt worden door zowel client als server.

Verklaring

Genereer **altijd** eigen Diffie-Hellman parameters! Gebruik niet de standaard parameters zoals deze zijn gedefinieerd in RFCs 2409, 3526, of 5114. Bijvoorbeeld Apache t/m 2.2 maakt hier gebruik van. Als eigen parameters niet in te stellen, gebruik dan **niet** de DHE ciphers.

Genereer altijd een DH sleutel welke tenminste dezelfde lengte heeft als de RSA privésleutel die gebruikt wordt voor het certificaat. De ciphersuite lijst is gebaseerd op de aangeraden configuratie van de Mozilla Foundation. Alleen de DSS gebaseerde ciphers zijn hier nog uit verwijderd aangezien deze inherent onveilig zijn (max 1024bit).

De ciphersuites welke zijn toegestaan of zelfs verplicht zijn, ondersteunen allen PFS. Hierdoor zijn de verstuurde versleutelde datastromen ook in de toekomst nog veilig, ook al zou onverhoopt toch een keer ergens een privésleutel uitlekken. Het verschil tussen traditionele versleuteling en "vluchtige" (ephemeral) versleuteling is dat in plaats van 1 sleutel voor alle versleutelde communicatie (de RSA privésleutel), er per communicatiesessie er een nieuwe sleutel (middels Diffie-Hellman) wordt gegenereerd. Deze sleutel is alleen geldig zolang deze sessie duurt. Na het verlopen van deze sessie heeft zowel de client als de server de sleutel niet meer en zal eventueel opgeslagen data uit de datastroom vrijwel onmogelijk nog teruggehaald kunnen worden. Ephemeral ciphersuites zijn te herkennen aan de suffix E in ECDHE en DHE.

Ciphers die niet op de toegestane lijst staan **mogen niet** gebruikt worden. Legacy ciphers waarbij gebruik gemaakt wordt van bijvoorbeeld RC4 of 3DES zijn onveilig en als vanzelfsprekend niet toegestaan te gebruiken. Lees meer over de problemen met RC4 en 3DES op respectievelijk in CVE-2015-2808 en in CVE-2016-2183

Wijziging ten opzichte van OSO'16

Toegevoegde ciphers:

1. Verplicht: ECDHE-RSA-CHACHA20-POLY1305
2. Optioneel: ECDHE-ECDSA-CHACHA20-POLY1305

Een nieuwe cipher is CHACHA20-POLY1305. De reden om deze toe te voegen is omdat niet alle hardware (goede) AES-NI ondersteuning heeft. Het gebruik van AES gebaseerde ciphers kan hierdoor voor systemen zwaarder zijn dan noodzakelijk. De cipher CHACHA20-POLY1305 biedt hierbij uitkomst door geen specifieke hardware ondersteuning te vereisen, maar wel veel lichter (en dus sneller) te zijn. Wanneer een server CHACHA20-POLY1305 aanbiedt naast de AES gebaseerde ciphers, kan een client besluiten om CHACHA20-POLY1305 te gebruiken omdat deze hem performancewinst oplevert.

Qua beveiliging doen CHACHA20 en AES niet voor elkaar onder. Beide cipher typen zullen ook hun weg vinden richting TLS1.3 waardoor deze toekomstvast zijn.

Ondersteuning binnen OSO is nog optioneel omdat niet alle TLS implementaties de cipher ondersteunen.

Verwijderde ciphers:

1. ECDHE-RSA-AES128-SHA
2. ECDHE-RSA-AES256-SHA
3. ECDHE-ECDSA-AES128-SHA
4. ECDHE-ECDSA-AES256-SHA
5. DHE-RSA-AES128-SHA
6. DHE-RSA-AES256-SHA

Alle ciphers die gebruik maken van een SHA1 signature zijn verwijderd.

Mogelijke oplossing

Eigen DH parameters zijn bijvoorbeeld te genereren middels openssl. Een werkende oplossing:

```
openssl dhparam -out dhparams.pem 2048
```

In Apache 2.4.8 en nieuwer kan vervolgens de file worden ingeladen.

```
SSLOpenSSLConfCmd DHParameters "{path to dhparams.pem}"
```

In sommige oudere versies van Apache kan ook de inhoud van dhparams.pem toegevoegd worden onderaan in het certificaat bestaand (appenden).
Lees meer voorbeelden op de deployment guide

Cipher volgorde

Eisen

- De server **moet** de cipher order bepalen
- De sterkste ciphersuite **moet** bovenaan de keuzelijst staan, aflopend naar de 'zwakste' onderaan de lijst

Verklaring

De server in een communicatieproces bepaalt uiteindelijk hoe sterk de versleuteling van de verbinding met de client wordt. De server wijst eventueel zelfs de verbinding met de client af als er geen sterke versleuteling tussen beide overeengekomen kan worden. De server moet dan ook garant staan voor de sterkst mogelijke configuratie die binnen OSO nodig wordt geacht. De server heeft een statische lijst met cipher suites die worden toegestaan en bepaalt hoe deze lijst in onderhandeling met de client wordt afgelopen. De sterkste match tussen server en client moet gekozen worden.
Binnen OSO worden alleen sterke ciphers toegestaan, echter is er ook nog een performance verschil tussen verschillende suites. Dit heeft voor zowel client als server impact, dus ook hier heeft de server, in opvolging van de OSO eisen, invloed op de keuze van de snelste ciphers.

Mogelijke oplossing

In Apache kan de cipher volgorde geforceerd worden middels

```
SSLHonorCipherOrder on
```

In IIS kan dit geregeld worden zoals beschreven in deze guide

Renegotiation

Eisen

- Secure renegotiation **moet** worden ondersteund
- Insecure client-renegotiation **mag niet** ondersteund worden
- Secure client-renegotiation **mag niet** ondersteund worden

Verklaring

Heronderhandeling over de TLS parameters mag nooit geïnitieerd worden vanuit de client, alleen vanuit de server. De server bepaalt of en zo ja wanneer dit moet gebeuren.

Compression

Eisen

- TLS compression **moet** uitgeschakeld zijn op de server en aan de client kant

Verklaring

In de meeste TLS modules is dit inmiddels functioneel al uitgeschakeld en daardoor onmogelijk te gebruiken. Mits dit toch bruikbaar is, is het voor een aanvaller mogelijk om achter geheime informatie te komen die versleuteld is in het berichten verkeer. De precieze werking gaat te diep voor deze wiki, maar is hier terug te lezen.

Sessie hervatting

Eisen

- Sessie hervatting **mag** ondersteund worden
- Sessie hervatting **kan** extra risico's met zich meebrengen, gebruik het alleen als bewuste keuze!

Verklaring

Sessie hervatting heeft als doel een stuk van de TLS handshake over te slaan omdat de sessieparameters aan zowel client als server kant in cache gehouden worden. Verbindingen tussen client en server die veelvuldig geopend en gesloten worden hebben hiermee een performance voordeel. Er dient wel rekening gehouden te worden met cachingtijden en de opslag van deze cache. Op het moment dat de sessie opgeslagen wordt, worden tijdelijke sleutels welke alleen gedurende de lifetime van de sessie bestaan toch gepersisteerd. Hierdoor is het mogelijk dat een derde deze cache op de server of zelfs een shared storage systeem kan uitlezen. Sessiesleutels kunnen hierdoor dan ook alsnog gecompromitteerd worden. Het veiligst doch traagst is het volledig uitschakelen van sessie hervatting.

ServerNameIndication

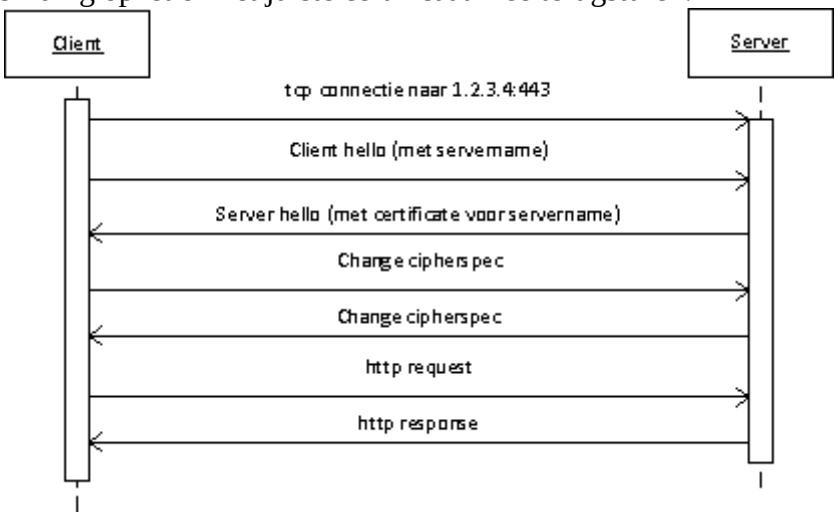
Eisen

- ServerNameIndication (SNI) **moet** door elk systeem dat acteert als client geïmplementeerd zijn
- ServerNameIndication (SNI) **mag** door elk systeem dat acteert als server geïmplementeerd zijn

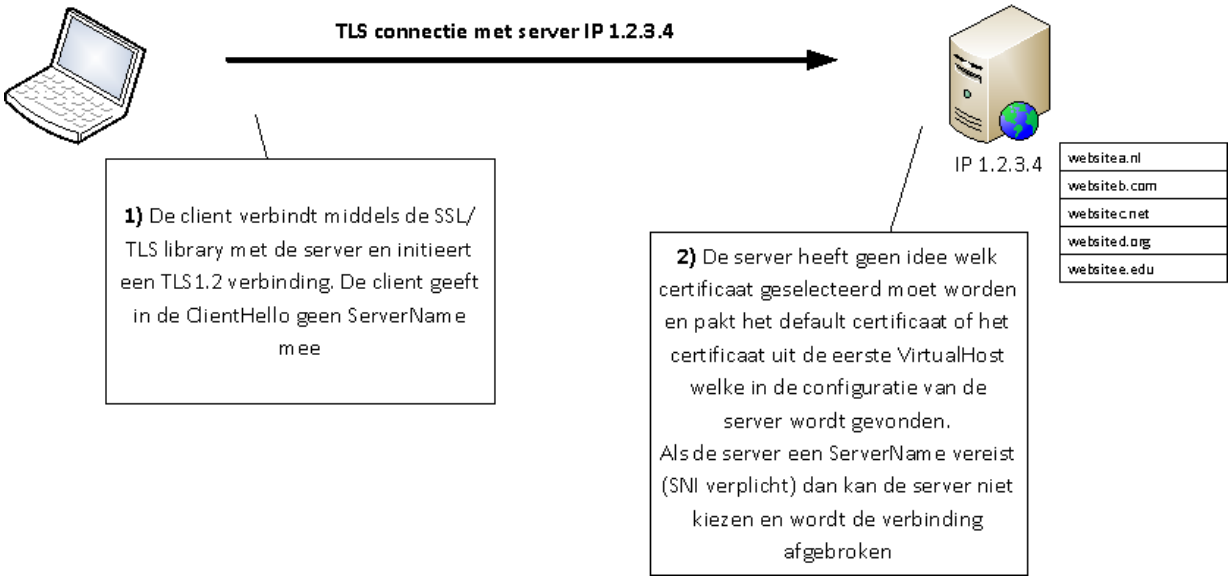
Verklaring

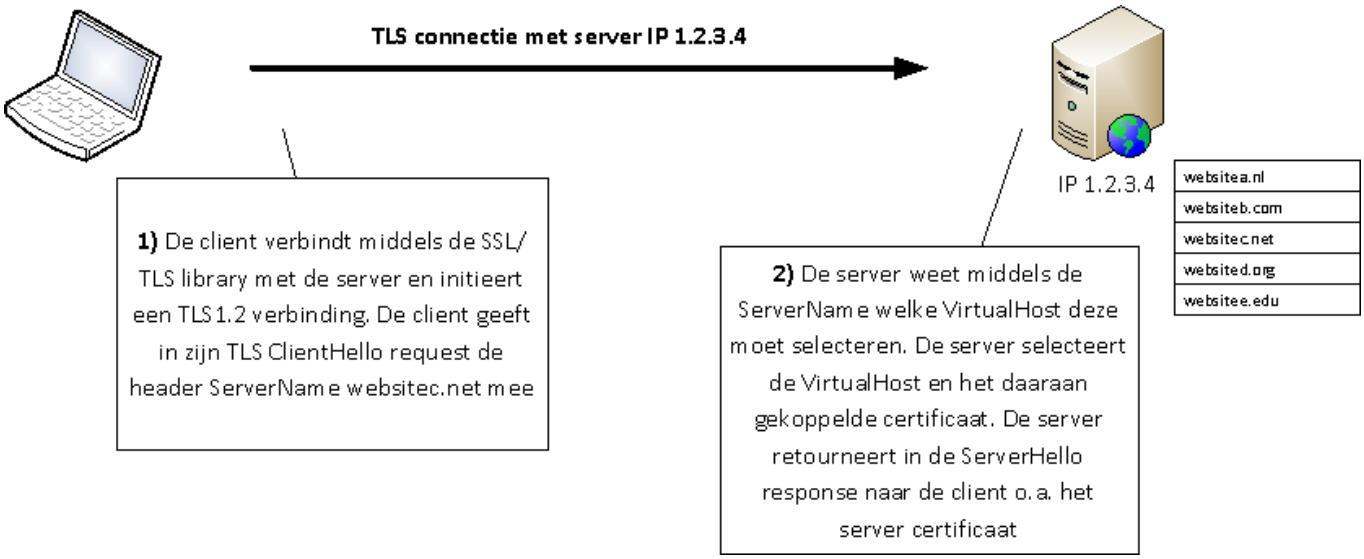
Een SSL certificaat wordt geïnstalleerd om een http verbinding te beveiligen. Hierbij wordt de volledige verbinding versleuteld op sessie niveau. Dit vindt plaats nog voordat er middels HTTP uitgewisseld is om welke hostname het gaat. Hierdoor is het voor de webserver onmogelijk om te bepalen voor welke domein het certificaat opgevraagd wordt. De webserver geeft het standaard certificaat of zelfs helemaal geen certificaat terug.
SNI zorgt ervoor dat op sessie niveau, tijdens het opzetten van de versleutelde verbinding, al

een extensie wordt meegestuurd met de hostname erin. TLS kan hierdoor bepalen voor welk certificaat een client de verbinding opzet en het juiste certificaat mee terugsturen.



Dit ziet er als hiernaast uit:
Elke client moet dit binnen OSO ondersteunen omdat er reeds leveranciers zijn die server-side SNI nodig hebben om het juiste certificaat te kunnen retourneren aan de client.
Ter illustratie schematisch weergegeven hoe de communicatiestroom er met en zonder SNI uitziet:
Zonder SNI:





Met SNI:
Weblinks over SNI-configuratie

- Artikel over het configureren van SNI op IIS 8 (Windows Server 2012)
- Artikel over het configureren van SNI op Apache2.x

Certificate Authorities (issuers)

Eisen

- In de TLS handshake fase is het **wenselijk** dat de server naar client een lijst met geaccepteerde CA's (issuers) teruggeeft

Verklaring

Het is in een communicatieproces wenselijk dat een server richting een client aangeeft wat er van deze wordt verwacht. Binnen TLS bestaat er in de handshake procedure de mogelijkheid de client middels het 'certificate_authorities' veld mee te geven welke certificaat leveranciers geaccepteerd worden als uitgever van het client certificaat. Een client kan hierdoor automatisch in de keystore het gewenste certificaat selecteren of juist vroegtijdig constateren dat het niet over een certificaat beschikt wat de server accepteert. Het veld is echter niet verplicht binnen TLS en zo ook niet voor de partijen binnen OSO.

Wanneer het veld gevoerd wordt door een server, moet het zich houden aan de lijst van leveranciers.

Het Traffic-center voert wel altijd het 'certificate_authorities' veld in de handshake.

Fallback SCSV (protocol downgrade attack prevention)

Eisen

- Fallback SCSV wordt **niet** geïmplementeerd

Verklaring

Het gebruik van Fallback SCSV is nuttig als er TLS protocol versie downgrades mogelijk zijn naar bijvoorbeeld TLSv1 of SSLv3. Binnen OSO is dit echter niet het geval. Alleen TLSv1.2 wordt toegestaan.

Public key pinning

Eisen

- Public key pinning wordt **niet** ondersteund

Verklaring

Public key pinning (Public key pinning / Linux Implementatie) is nog experimenteel en wordt voornamelijk door een aantal browsers ondersteund. Het zal in de toekomst mogelijk wel een eis gaan worden als ook andere software bibliotheken de pinning controle gaan uitvoeren.

informatiebeveiliging per interactie

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

Versturen Notificatie	• Bronsysteem verifieert het servercertificaat van Doelsysteem. • Doelsysteem verifieert het clientcertificaat van het Bronsysteem. • Bronsysteem en Doelsysteem versleutelen de verbinding. • Bronsysteem logt de interactie. • Doelsysteem logt de interactie.
Pingen Traffic Center	• Systeem verifieert servercertificaat van het Traffic Center. • Traffic Center verifieert het clientcertificaat van het Systeem. • Systeem en Traffic Center versleutelen de verbinding. • Traffic Center logt de interactie.
Registreren Aanleverpunt	• Systeem verifieert servercertificaat van het Traffic Center. • Traffic Center verifieert het clientcertificaat van het Systeem. • Systeem en Traffic Center versleutelen de verbinding. • Traffic Center logt de interactie.
Controleren van de APsleutel	• Systeem verifieert servercertificaat van het Traffic Center. • Traffic Center verifieert het clientcertificaat van het Systeem. • Systeem en Traffic Center versleutelen de verbinding. • Traffic Center logt de interactie.

Het valideren van de certificaten zou geen onderdeel moeten zijn van de Business Logica van een LAS- of RP- applicatie, maar zou onderdeel moeten zijn van de onderliggende infrastructuur die wordt gebruikt bij het opzetten van de verbinding. De webserver (IIS/Apache/soortgelijk) dient deze taak uit te voeren en moet hiervoor geconfigureerd worden.

Het configureren en plaatsen van de publieke sleutels op een webserver is per type/smaak webserver verschillend. Het is lastig om hier een ?algemeen OSO recept? voor te geven. Normaliter is dit geen taak van ontwikkelaars maar van applicatie- of server- beheerders. Het maakt derhalve geen onderdeel uit van de use-case beschrijvingen. Er wordt reeds van uit gegaan dat TLS en certificaat validatie op een ander niveau gedaan is.

controle procedure

Controle procedure naleving beveiligingseisen

De implementatie engineer bij Kennisnet zal naleving van de in het PvE genoemde eisen controleren. Deze controle bestaat uit de jaarlijkse kwalificatie na oplevering van de nieuwe functionaliteiten en eisen, ontwikkeld in het kader van OSO. Daarnaast zal de implementatie engineer periodiek steekproeven houden om de kwaliteit van OSO keten te waarborgen. Deze tests verlopen middels voorgeschreven scripts, waardoor er een uniforme controle uitgevoerd kan worden.

De testprocedure bestaat uit minimaal een:

- Functionele test: werkt de koppeling tussen LAS en TC en tussen LAS en LAS zoals voorgeschreven
- Technische test: worden alle beveiligingseisen zoals opgenomen op deze wiki daadwerkelijk correct uitgevoerd

Technische test

In hoofdlijnen opgesomd wat er binnen de technische test gecheckt wordt:

- Klopt het server certificaat van het systeem waarop het aanleverpunt wordt aangeboden?
    - Is het certificaat nog geldig?
    - Komt servername in het certificaat overeen met de domeinnaam in de url?
    - Is het certificaat en de certificaatketen te valideren tegen het root CA certificaat?
    - Is het certificaat niet ingetrokken (revoked) door de CA?
    - Welke hash signatuur wordt er gebruikt?
- Wordt SNI gesupport?
- Wat voor private key wordt er gebruikt en met welke sleutellengte?
- Geeft de server aan in de TLS handshake of deze bepaalde client certificaten verwacht?
- Ondersteunt de server 'secure renegotiation'?
- Ondersteunt de server 'secure client-initiated renegotiation'?
- Ondersteunt de server 'insecure client-initiated renegotiation'?
- Ondersteunt de server OCSP stapling?
- Ondersteunt de server serverside cipher ordering?
- Ondersteunt de server TLS compression?
- Ondersteunt de server session resumption caching?
- Ondersteunt de server session resumption tickets?
- Ondersteunt de server SCSV fallback?
- Ondersteunt de server HSTS?
- Is de server vatbaar voor de CCS vulnerability?
- Is de server vatbaar voor TLS poodle?
- Is de server vatbaar voor Heartbleed?
- Accepteert de server alleen de voor OSO geaccepteerde client certificaten?
    - Test met een PKIoverheid certificaat

    - Test met een random ander client certificaat verkregen uit een legitieme CA in de markt
    - Test met een self-signed certificaat
- Welke TLS/SSL protocollen ondersteunt de server?
- Welke ciphersuites ondersteunt de server?

Procedure bij (vermoeden van) misbruik

Procedure bij (vermoeden van) misbruik

- Bij een vermoeden van en zeker bij geconstateerd misbruik, **moet** er direct contact opgenomen worden met Kennisnet Support
- Op het moment dat geconstateerd wordt dat er ergens in de keten problemen zijn met de beveiliging, **moet** er direct contact opgenomen worden met Kennisnet Support

geldigheid

Geldigheid van de beveiligingseisen

De eisen gelden de gehele periode waarin het bovenliggende PvE geldt. De eisen worden opgesteld in aanloop naar de publicatie van een nieuw PvE. Normaliter geldig gedurende een geheel schooljaar. De eisen worden tezamen met de rest van het PvE vastgesteld door het Technisch Overleg waarna deze niet meer gewijzigd zullen worden.

Er is echter een uitzondering hierop. Deze wordt van kracht als blijkt dat gedurende de periode voorafgaand aan het effectief worden van de eisen dan wel gedurende de looptijd van de eisen er zich nieuwe beveiligingssituaties ontwikkelen die aanpassing vereisen. Deze nieuwe eisen worden voor doorvoering ter vaststelling voorgelegd aan het Technisch Overleg, tenzij er bepaald wordt door de Security Officer van Kennisnet dat deze nieuwe eisen een hoge urgentie vormen. De Security Officer van Kennisnet zal op dat moment een risico analyse doen en bepalen welke aanpassingen er per direct noodzakelijk zijn. Deze worden gecommuniceerd over de Techlijst van OSO. In het daarop volgende Technisch Overleg zullen de maatregelen geevalueerd worden en opnieuw worden vastgesteld dan wel aangepast.

FAQ

Het is onduidelijk hoe de 'SAAS certificaten' werken als één (1) leverancier meerdere SaaS applicaties aanbiedt

Moet iedere applicatie dan hetzelfde certificaat gebruiken? Houdt dat dan ook in dat iedere applicatie op dezelfde URL (er van uitgaande dat dat bedoeld wordt met ?internetadres? in de memo) dient te worden aangeboden? Dit levert ons inziens ongewenste risico?s op.
De naam 'SAAS certificaat' dekt niet geheel de lading, maar is ondertussen dermate breed gebruikt dat het waarschijnlijk meer problemen dan verduidelijking oplevert om de naamgeving aan te passen. Afhankelijk van de situatie kan het nodig zijn dat een Leverancier meerdere certificaten hanteert. Er moeten in dat geval meerdere certificaten worden aangeschaft. In de uitgegeven certificaten wordt dan aan het OIN/HRN een opvolgend nummer (001, 002, etc.) toegevoegd.
Als een Leverancier meerdere pakketten levert die op OSO aangesloten worden, dan zijn er twee aanpakken mogelijk:

- Beide pakketten maken gebruik van hetzelfde 'SAAS certificaat'. Aangezien de url per Aanleverpunt wordt geregistreerd, is het mogelijk om met meerdere pakketten binnen OSO te werken onder de vlag van dezelfde Leverancier.
- Elk pakket heeft zijn eigen 'SAAS certificaat'. In de OSO administratie wordt dan ingericht alsof er twee 'losse' Leveranciers zijn. Afhankelijk van organisatorische en/of juridische eisen kan een van deze twee aanpakken de voorkeur krijgen.

Een derde variant is als een School zelf een Systeem 'levert', bijvoorbeeld door in een eigen (private) cloud een applicatie van een Leverancier te hosten. In dat geval kan niet het certificaat van de Leverancier worden gebruikt en moet de School zelf een certificaat gebruiken. Binnen de OSO administratie krijgt de School dan ook de rol van Leverancier (voor haar eigen systeem).

Welke stappen moet ik als 'OSO 15 leverancier' doen om met 'SAAS certificaten' te gaan werken?

De nieuwe PKI inrichting heeft een aanzienlijke impact op de beveiliging van OSO.
Hieronder worden op hoofdlijnen de acties opgesomd die een Leverancier moet nemen:

1. Aanvragen PKIoverheid-certificaat bij een geaccrediteerde certificatiedienstverlener
2. Alle systemen: Installeren SAAS certificaat op eigen infrastructuur
3. Bronsysteem: aanpassen controle van certificaat van Doelsysteem bij Dossier aanvraag
4. Doelsysteem: toevoegen controle van certificaat van Bronsysteem bij ontvangst Notificatie

Blijven de huidige Aanleverpunten geldig/actief?

De huidige Aanleverpunten kunnen als 'actief' geregistreerd blijven zowel in de Schoolsystemen als in het TC/Register. Er is **geen** gebruikershandeling nodig na het verwijderen van het AP-certificaat. Wanneer een eindgebruiker in het Aanleverpunt een wijziging invoert (en bij het aanmaken van een nieuw Aanleverpunt) moet het Schoolsysteem het Aanleverpunt (opnieuw) registreren. (Waarbij optioneel ook de AP-sleutel moet worden gecontroleeerd.)

Hoe moet op Windows(IIS) servers TLS geconfigureerd worden

Het blijkt dat de correcte configuratie van tweezijdige TLS op Windows systemen in de praktijk lastig is. Wij hebben uit laten zoeken hoe dit geconfigureerd moet worden en hiervoor een stappenplan op laten stellen. Dit stappenplan is hier te vinden.

Implementatie 'work around' TLS op .NET niet (altijd) mogelijk

De 'work around' configuratie geeft een optie om TLS 1.2 niet op server maar op applicatie niveau af te dwingen. In de praktijk blijkt deze aanpak in .NET niet(!) te implementeren op dit moment.

De reden hiervoor is dat het niet mogelijk is om in een webapplicatie die binnen IIS draait om het niveau van een TLS 1.2 verbinding te controleren. Omdat een netwerk verbinding in IIS tot stand gebracht wordt (OS niveau) kan op applicatie niveau niet gekeken worden naar de de verbinding. De applicatie kan alleen kijken naar de data die over de verbinding verstuurd wordt.

Helaas maar inderdaad dat is wat ik in de vakantieperiode ook ben tegengekomen. Er zijn geen mogelijkheden om bijv. een global variabele in IIS te vullen met de TLS session metadata. Het is voor een .NET app achter IIS niet mogelijk om achter die TLS gegevens te komen. Hier wordt beschreven hoe IIS omgaat met SSL/TLS (iets dan andere servers).

OSO:Releases

Deze pagina geeft een overzicht van de OSO versies.

datum	omschrijving	PvE/Ontwerp in PDF	toegepaste dossier standaard	WSDL	live datum
20170800	OSO'17		2017.1	**RC1: 20170309**	2017080
20160411	Bijgewerkt ontwerp na eerste ontwikkelsprint TC'16	Bestand:OSO'16 PvE.20160411.pdf	[Edustandaard OSO 2016.1]	Bestand:Overstap.20160401.wsdl.zip	2016041 (Sandbox
20160226	Vastgesteld Programma van Eisen/Ontwerp OSO'16	Bestand:OSO'16 PvE.20160226.pdf	[Edustandaard OSO 2016.1]	Bestand:Overstap.20160309.wsdl.zip	201608 ?
2015-02	OSO'15		[EduStandaard OSO 1.2.2]		201507x
2014-02	Fase 2B		[EduStandaard OSO 1.1.1]		2014070

Index

Index

Use cases OSO'17

- Algemene eisen aan aangesloten systemen
- Inhoudelijke eisen aan aangesloten systemen
- Functionele eisen per type systeem

- Pingen van Traffic Center
- Registreren van een Aanleverpunt
- Controleren van de AanleverpuntSleutel
- Opvragen van Aanleverpunten

- Uitvoeren van een opvraag Sessie
- Initiëren van een Sessie
- Opvragen van een Dossier
- Controleren van een Sessie
- Importeren en tonen van een Dossier
- Afmelden van een Sessie

- Versturen Notificatie
- Versturen NotificatieMelding naar TC
- Versturen Notificatie naar Doelsysteem

- Samenstellen van het Dossier
- Selectief samenstellen van Dossier
- Tonen Dossier aanvragen (kleine Notificatie)
- Laten inzien Dossier door ouders
- Registratie inzage Dossier (door ouders)
- Dossier klaarzetten voor Scholen
- Dossier controleren tegen OSO standaard

- Verwerken opstaande Dossier aanvragen
- Tonen ontvangen Dossier aanvragen
- Tonen ontvangen Notificaties

- Uitwisseling met Samenwerkingsverbanden
- Aanleverpunt selecteren voor Notificatie
- Versturen TerugkoppelingMelding naar TC
- Versturen Terugkoppeling naar Bronsysteem
- Tonen overzicht binnengekomen Dossiers

- OSO:2017/Beveiliging
- OSO:2017/Beveiliging/FAQ
- OSO:2017/Architectuur

- OSO:2017/Leeswijzer
- Wijzigingen in OSO'17

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.
KoppelSleutel	Koppelsleutel is een random identificatie kenmerk, alleen	De koppelsleutel wordt door het TC gegenereerd voor het

woord	verklaring	toelichting
	bekend en geldig voor één specifiek dossier bij twee betrokken systemen.	aanvragen van een aanvraagdossier ten behoeve van de overdracht tussen school/instelling en Samenwerkingsverband Passend onderwijs, en voor de terugkoppelingen op deze aanvragen. De koppelsleutel is NIET gebaseerd op PGN of ander persoonskenmerk.
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.
OV	Overdracht	Aanduiding voor het doel van een Notificatie of Aanleverpunt.
PaO	Passend Onderwijs	Aanduiding voor het doel van een Notificatie of Aanleverpunt.
PGN	PersoonsGebonden Nummer	Binnen OSO wordt het PGN toegepast als sleutel bij het opvragen van een Dossier. Een PGN is ofwel het Burger

woord	verklaring	toelichting
		Service Nummer (BSN) ofwel het Onderwijsnummer van de desbetreffende leerling.
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.
Samenwerkingsverbandsysteem Passend Onderwijs	Een (regionale) samenwerking van scholen in het PO of het VO. Alle scholen voor regulier en speciaal onderwijs zijn aangesloten bij een (of meerdere) samenwerkingsverband(en).	Scholen zijn aangesloten op Samenwerkingsverbanden Passend Onderwijs om de regelingen rond de wet Passend Onderwijs uit te voeren.
Samenwerkingsverbandsysteem (SWV)	Een informatiesysteem gedeeld door scholen van een Samenwerkingsverband dat ook door het Samenwerkingsverband Passend Onderwijs wordt gebruikt.	SWV's en RP's kunnen via OSO Dossiers uitwisselen in het kader van een aanvraag door een School bij een Samenwerkingsverband.
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.