Overstap Service Onderwijs

Programma van Eisen ‘16

Versie: 20160226

Inhoud

OSO:2016

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 diverse partijen samen om de overdracht van leerlinginformatie tussen scholen te optimaliseren. De daadwerkelijke overdracht van dossiers verloopt volgens use cases die hieronder beschreven worden. Per use case vinden een aantal interacties tussen systemen plaats. De beschrijving van use cases en interacties is hier te vinden. Een belangrijk aandachtspunt van OSO is de beveiliging van de gegevens, de maatregelen die hiervoor voorgeschreven worden, zijn uitgewerkt in beveiliging.

Voor inhoudelijke vragen kunt u contact opnemen met OSO-support.

OSO specificatie

- Leeswijzer
- Wijzigingen in OSO'16
- OSO beveiligingsvoorschriften en -maatregelen
- Index
- Recente wijzigingen

Use Cases

- Als systeem(bouwer) wil ik op OSO aansluiten
- Als systeem(bouwer) wil ik weten welke omgevingen er zijn
- Als systeem(bouwer) wil ik mijn OSO aansluiting testen
- Als systeem(bouwer) wil ik met een testschool uitwisselen

Hotlinks

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

Communicatie

Overstap Service Onderwijs site

Atom Feed wijzigingen OSO wiki

leeswijzer

Architectuur

Onderwerp	Opmerkingen
Algemeen	
Systeemlandschap	
Uitwisselproces	
Beveiliging	
Algemene eisen en richtlijnen	

In de wiki wordt in de Use Case pagina's onderscheid gemaakt tussen organisatorisch en technisch niveau om lezers snel toegang te geven tot voor hen relevante informatie. Beschrijvingen van stappen of use cases in het OSO proces hebben daarom opgedeeld in

- een algemeen beschrijvende pagina
- pagina's met beschijvingen van deelstappen in het proces
- pagina's die per deelstap het scenario en bijbehorend berichtenverkeer beschrijven.

Use cases voor alle systemen

Algemeen	(Deel)processtap	Use case	Opmerkingen
Aanroep voor het esten van de beschikbaarheid van het Traffic Center		'Pingen' van Traffic Center	
Registreren vanuit een Systeem van een Aanleverpunt in het Register	Bij het registreren van een Aanleverpunt kan met het controleren van de APsleutel de invoer van de eindgebruiker gevalideerd worden.	Registreren van een OSO Aanleverpunt	Voorwaarde voor uitwisselingen met OSO voor Bron- én Doel-systemen
Valideren van de invoerde waarden in een Systeem bij een Aanleverpunt op basis van de Aanleverpuntsleutel.		Controleren van de APsleutel	Optioneel: Geen verplichting om deze aanroep te implementeren

Use cases voor Bronsystemen

Algemeen	(Deel)processtap	Use case	Opmerkingen
	Laten inzien Dossier	Registreren inzage	Vindt plaats 'binnen' systeem, geen directe interactie met OSO
Samenstellen Dossier		Controleren Dossier tegen standaard	Controleren van formaat en syntax van Dossier tegen EduStandaard Gegevensset OSO
		Dossier gereed zetten voor opvragen door Doelsysteem	Voordat Doelsysteem Dossier kan opvragen moet in Bronsysteem aangegeven worden dat Dossier gereed is en beschikbaar voor specifieke scho(o)l(en)
	Verwerken openstaande verzoeken		Vindt plaats 'binnen' systeem, geen directe interactie met OSO
Klaarzetten Dossier	Versturen Notificatie	Melden Notificatie	Na klaarzetten Dossier voorafgaand aan verzenden van Notificatie
		Notificatie versturen naar Doelsysteem	Melden aan Doelsysteem dat Dossier beschikbaar is gekomen
Overdragen Dossier		Controleren sessie	Na ontvangst van verzoek tot levering van Dossier
		Reageren op verzoek tot levering Dossier	Als antwoordende partij bij Opvragen Dossier

Use cases voor Doelsystemen

Algemeen	(Deel)processtap	Use case	Opmerkingen
		Aanvragen Sessie	Eerste stap bij het opvragen van een Dossier
		Opvragen Dossier	Als antwoordende partij bij Opvragen Dossier
Overdragen Dossier	Uitvoeren opvraag Sessie	Importeren van ontvangen Dossier	Na een geslaagde overdracht
		Afmelden van de Sessie	Na het ontvangen van een Dossier of het aflopen van de Aanleverpunten
Klaarzetten Dossier		Ontvangen van een Notificatie	Als geaddresseerde van een Notificatie

2016-08

Het Programma van Eisen/Ontwerp van OSO'16 is op de wiki te vinden: OSO '16 Voornaamste wijzigingen zijn de nieuwe PKI infrastructuur en het Notificatie mechanisme.

- De voorstellen tot functionele wijzigingen in OSO'16 zijn beschreven in: Bestand:Wijzigingsvoorstellen OSO'16 Def 20151112.pdf.
- Het voorstel voor het herzien van de PKI infrastructuur is beschreven in: Bestand:Memo Voorstel wijzigen PKI infrastructuur.pdf.

Hieronder volgen de wijzigingen in OSO'16 (ten opzichte van OSO'15):

Netwerk/infra/beveiliging

- PKI Infrastructuur ('SAAS certificaat') In OSO'16 wordt de overstap gemaakt van 'Aanleverpunt certificaten' naar 'SAAS certificaten'. Dit betekent een grote aanpassing aan de manier waarop de beveiliging is geregeld binnen OSO. Het is daarom niet mogelijk hier kort aan te geven welke wijzigingen hiervoor nodig zijn.
- Aanvullende eis aan logging De logging van systemen moet voldoende informatie bevatten om vast te kunnen stellen welke 'account' de opdracht gaf een dossier op te halen of een dossier beschikbaar stelde.

Functioneel

De functionele aanpassingen zoals voorgesteld in het memo van 2015112:

1. Notificatie mechanisme Dit is een nieuwe functionaliteit die zowel Bron- als Doel- systemen raakt. Doelsystemen moeten nu altijd een URL registreren bij het Aanleverpunten waarnaar de Notificatie gestuurd kan worden.
2. Gebruiken van timestamp (dossierVerzameldatum) bij het opvragen van een Dossier aanvraag; dit heeft impact op Opvragen van een Dossier én Samenstellen van een Dossier. Bestaande Bronsytemen moeten deze parameter kunnen verwerken, Doelsystemen kunnen er voor kiezen deze mogelijkheid beschikbaar te maken aan hun eindgebruikers.
3. Tonen van binnengekomen gegevens en bijlagen: Doelsystemen moeten de inhoud van het ontvangen Dossier tonen aan Eindgebruikers.
4. Optie om specifiek AP te bevragen ('Optioneel ondersteunen Speciaal Onderwijs'): Deze functionaliteit maakt het mogelijk voor Doelsystemen om uitwisselingen tbv Specaal Onderwijs te ondersteunen. Dit is een optionele uitbreiding, het staat Leveranciers vrij om dit in te bouwen. Er is geen impact voor Doelsystemen.
5. Aanpassing adressering In OSO'16 krijgen worden in alle berichten altijd vier adresvelden (BronBRIN, BronAPindex, DoelBRIN, DoelAPindex) gebruikt. Voor aangesloten systemen betekent dit dat de aanroepen naar het TC en onderling zullen wijzigen (volgorde van velden en extra velden). Functioneel is er geen wijziging.

Aanvullende aanpassingen:

- Apindex naar 3 digits. Doordat de BRIN-APindex combinaties niet hergebruikt worden, lopen we langzaam uit de huidige index die twee digits groot is. Alle systemen worden hierdoor (licht) geraakt.
- AP verificatie met sleutel*
    - Orgineel voorstel uitbreiding functionaliteit met APsleutel: Bestand:Uitbreiding OSO functionaliteit met APvalidatie 20160210.pdf
- Aanpassing zoeksleutel. Het certificaat dat gebruikt wordt bij het genereren van de zoeksleutel wordt vervangen met een nieuw in OSO'16 dat wordt uitgegeven door Kennisnet.
- Controle op geldige Dossierversie/nieuwe foutmelding: Bronsystemen moeten als een Dossier wordt opgevraagd, controleren of dit de geldige versie heeft van de Dossierstandaard. Als dit niet het geval is, moet een nieuwe foutmelding worden teruggegeven naar het Bronsysteem én moet dit getoond worden aan de Eindgebruiker van het Bronsysteem in het overzicht van binnengekomen Dossier verzoeken.

* Onder voorbehoud: Nog te bespreken tijdens Technisch Overleg 20160216

Architectuur

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.

Maximalisatie van import

Bij het importeren van een Dossier wordt gestreefd naar het voorkomen van informatieverlies. Een Doelsysteem dat een Dossier ontvangt moet streven om zoveel mogelijk velden uit het Dossier over te nemen in het Doelsysteem en waar mogelijk als bewerkbaar veld. Wanneer er sprake is van meervoudige levering, dan moet het Doelsysteem zorg dragen dat door de eindgebruiker aangepaste velden niet of na toestemming van de eindgebruiker wordt overschreven.

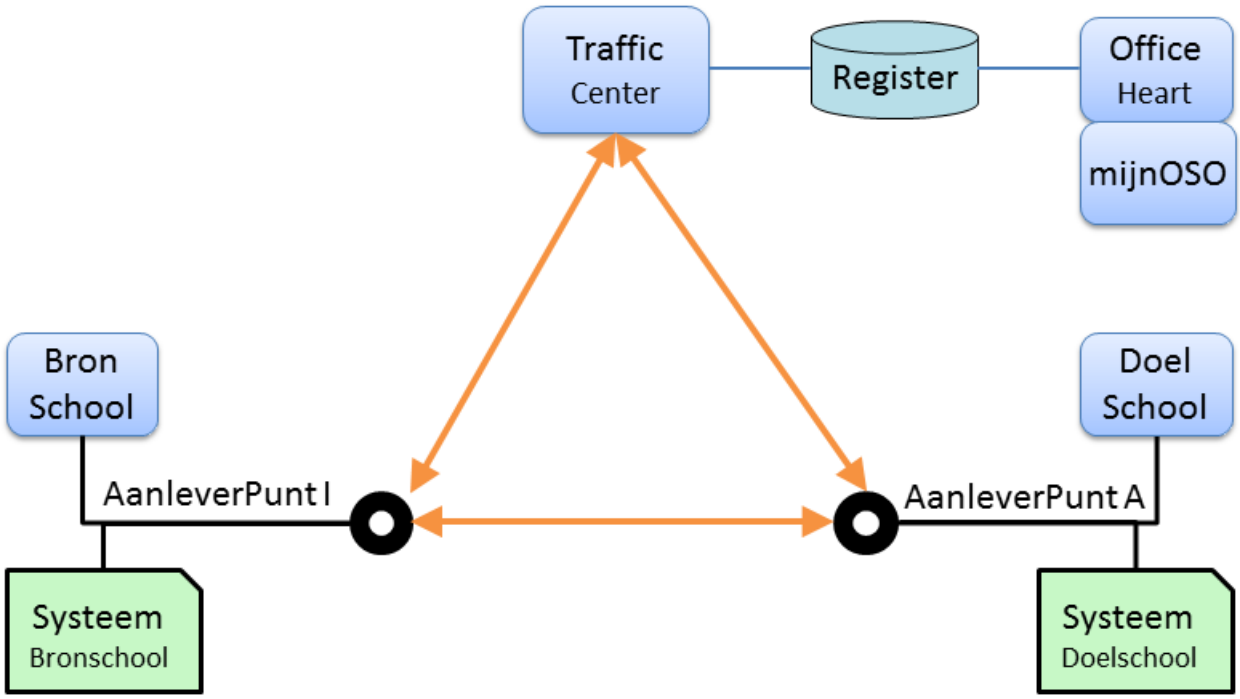
Dossierformaat

Binnen OSO wordt gewerkt met één gestandaardiseerd formaat voor het Dossier; in OSO'16 wordt de Standaardversie: **2016.1** gebruikt. Een Bronsysteem moet voorafgaand aan verzending controleren dat het Dossier hieraan voldoet.

Architectuur

Systemen

De Overstapservice faciliteert het digitaal uitwisselen van dossiers (of 'OKR") tussen systemen van scholen. Een dossier wordt van een systeem van de huidige school, de Bronschool, verzonden naar een systeem van de Doelschool. Om dit transport te faciliteren is een stelsel van afspraken en systemen opgezet, dat in de figuur hieronder schematisch is weergegeven. Hierin zijn de volgende componenten te onderscheiden:



School

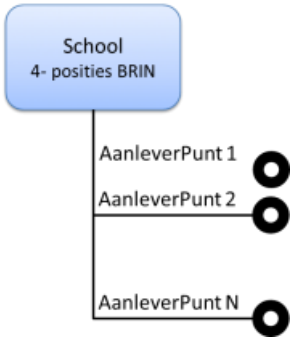
Een school of instelling kan meerdere systemen gebruiken om gegevens van leerlingen te registreren en te verwerken, soms verspreid over meerdere vestigingen. Al deze systemen kunnen aangesloten worden op OSO. Per school moet voor ieder systeem dat wordt aangesloten een AanleverPunt (AP) gedefinieerd worden. Via haar AP koppelt een systeem met OSO en kan de school gegevens uitwisselen met andere OSO deelnemers.

Bron en doel- school

Binnen een uitwisseling is er altijd één school, de Doelschool, die één dossier bij één Bronschool opvraagt.

Aanleverpunt

Binnen OSO wordt iedere combinatie van school(vestiging) en het op de school gebruikte systeem geregistreerd zodat dossiers van en naar het juiste schoolsysteem verstuurd kunnen worden. Een dergelijke koppeling van schoolsysteem met OSO wordt aanleverpunt (AP) genoemd.



School met aanleverpunten

Een Aanleverpunt wordt gekoppeld aan een school op bestuursnivo (ook wel BRIN of BRIN(4) nivo genoemd). Een Aanleverpunt kan binnen OSO alleen Dossiers ophalen of aanbieden voor het geregistreerde BRIN(!).

Naast de BRIN heeft een Aanleverpunt een index die samen met de BRIN de unieke sleutel van de AP vormt. Het eerste AP van een school heeft index '000', daarna wordt er door genummerd ('001', '002', etc.) Deze nummering heeft geen betekenis afgezien van de identificatie van het Aanleverpunt. (De AP index heeft **geen** relatie met door DUO of de inspectie toegekende nummers aan vestigingen of met het OIN.) Een AP heeft een label dat bij registratie wordt ingevuld en een aanduiding of het een LAS of RP betreft.

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

Systeem

Aangesloten systemen kunnen de rol vervullen van bron- of doel -systeem. Eenzelfde LAS of RI-platform kan zowel de rol 'documentbron' als de rol 'documentdoel' vervullen, maar nooit in dezelfde uitwisselsessie. Afhankelijk van het systeem zal het geschikt zijn om als bron of doel te vervullen voor bepaalde typen uitwisseling.

Traffic Center

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

Binnen het Traffic Center kunnen de volgende componenten worden onderscheiden:

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

Register

In het Register wordt iedere combinatie van school(vestiging) en het op de school gebruikte systeem geregistreerd als een Aanleverpunt. Het beheer van de Aanleverpunten wordt door Schoolbestuurders uitgevoerd in het mijnOSO-portaal. Scholen zijn zelf verantwoordelijk voor het correct aangeven welke Leverancier(s) namens hen Dossiers mogen aanbieden of opvragen. Het Traffic Center raadpleegt het Register als een Schoolsysteem een Dossier wil opvragen:

- Het Doelsysteem wordt tegen het Register gecontroleerd wanneer het een Sessie initieert om een Dossier op te vragen
- Een tweede controle op het Doelsysteem én de gegevens in het DocumentRequest bij de Sessie Controle aanroep van het bevraagde Bronsyteem.

Het Register bevat ook een log van alle transacties zoals die binnenkomen. Deze worden doorgeleverd voor rapportage doeleinden.

OfficeHeart/mijnOSO

- OfficeHeart is de backoffice van OSO. Hierin worden Leveranciers en Scholen geregistreerd en het kwalificatieproces geadministreert.
- mijnOSO is het portaal voor Scholen. Hierin kunnen schoolbestuurders de Aanleverpunten van hun scho(o)len beheren en aangeven welke Leverancier(s) namens hen optreden binnen OSO.

Kennisnet Validatie Service

De Kennisnet Validatie Service is een (formeel los van OSO staande) service voor het valideren van een Dossier tegen de EduStandaard OSO.

Proces

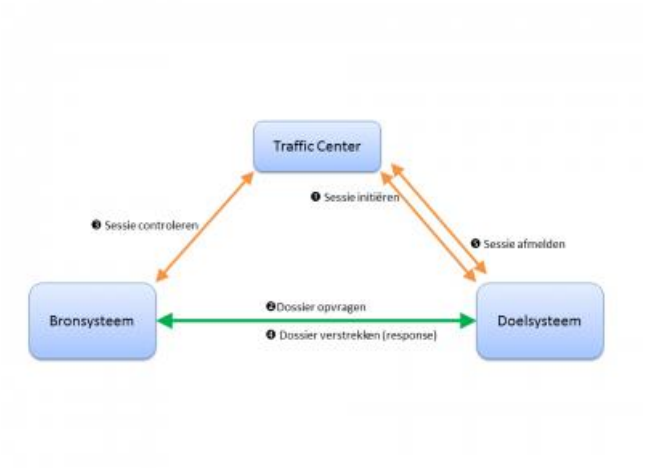
Berichten verkeer

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.

PGN en 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.

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.

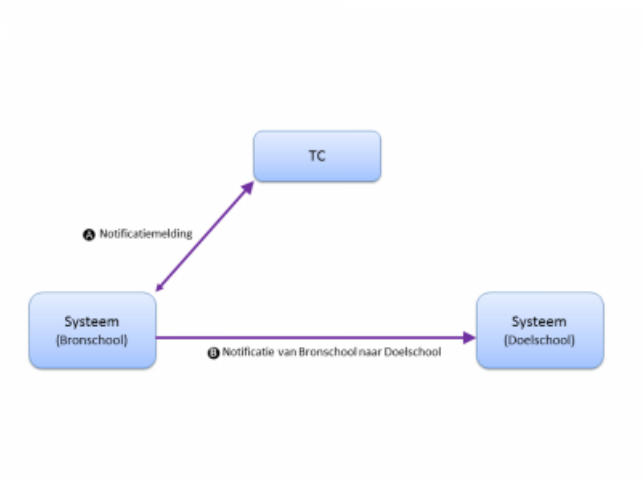
   Dit verzoek bevat het versleutelde BSN en de sessie id uit bericht 2. Het TC controleert deze gegevens; wanneer deze overeenkomen met een uitgegeven nog niet verlopen sessie wordt een ok teruggegeven (SessiecontroleResponse). Controleren sessie

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

Notificatie



In de figuur worden de stappen en berichten weergegeven die bij een succesvolle Notificatie 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.

Beveiliging

Toelaten partijen in keten

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 NOG DOEN te vinden.

Aangesloten leveranciers

- Overzicht systemen aangesloten op OSO

Certificaten

In OSO'16 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(!).
    - 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

Algemene eisen

Algemene eisen en randvoorwaarden

Bewaartermijn

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

Het verzonden overstapdossier dient twee jaar te worden bewaard. Voor een leerling die is doorverwezen naar een school voor Speciaal Onderwijs geldt een bewaartermijn van drie jaar voor het overstapdossier.

Na deze twee jaar dient het overstapdossier te worden vernietigd

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

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).

Overige technische randvoorwaarden

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)**

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

- 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.
- Een systeem registreert logregels voorzien van datum en tijd, met een nauwkeurigheid van ten minste 1 seconde.

- Een systeem garandeert een maximale afwijking van de UTC + 01:00 tijd (de tijdzone waarin Nederland valt) van 5 seconden.
- Log regels bevatten altijd het geldige sessie-id (wanneer dit is toegekend).
- Logregels voor de gebruiker kunnen na creatie niet worden aangepast of verwijderd.
- Logregels voor de gebruiker worden duurzaam bewaard en beschermd tegen verlies en verandering tot 2 jaar 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(!).

Aanleverpunt Registreren

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

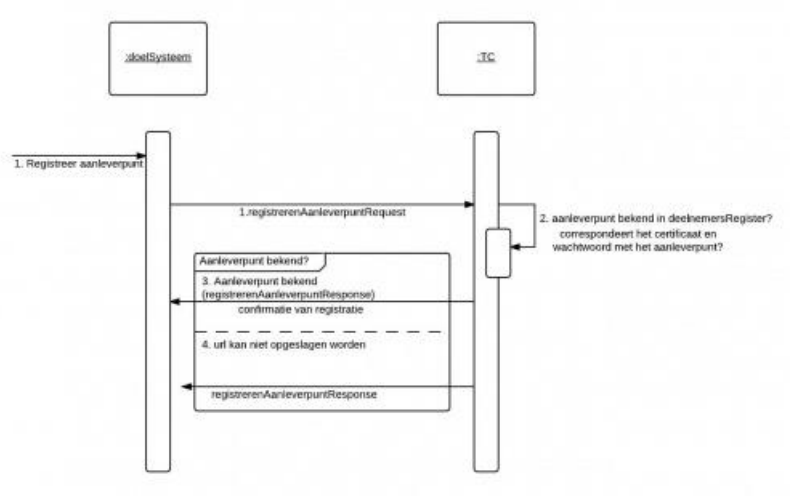
1. Een Schoolsysteem verstuurt een registreer Aanleverpunt request naar het Traffic Center.
2. Het Traffic Center controleert of het Aanleverpunt bekend is in het Register en of het Schoolsysteem gemachtigd is om de url van dit Aanleverpunt te registreren.
3. **If** Aanleverpunt geregistreerd mag worden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

Overzicht meldingen

Resultaat	**Type flow (N, A, E)**	**Omschrijving**
RegistratieGelukt	N	De URL is geregistreerd voor het aanleverpunt
AanleverpuntOnbekend	E	Het gebruikte certificaat komt overeen met het aanleverpunt in de registreerAanleverpuntRequest, maar het aanleverpunt is (nog) niet aangemaakt in het Traffic Center. Als men in mijn OSO een aanleverpunt handmatig toevoegt, dan wordt het aanleverpunt middels een synchronisatie proces aangemaakt in het Traffic Center. Het duurt meestal een aantal minuten voordat het aanleverpunt ook daadwerkelijk aangemaakt is in het Traffic Center.
OngeldigeURL	E	De URL die meegegeven werd in het registreerAanleverpuntRequest is niet valide.
SysteemOnbekend	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.
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.

- Response:

Sequence diagram Registreren Aanleverpunt



Traffic Center Pingen

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:

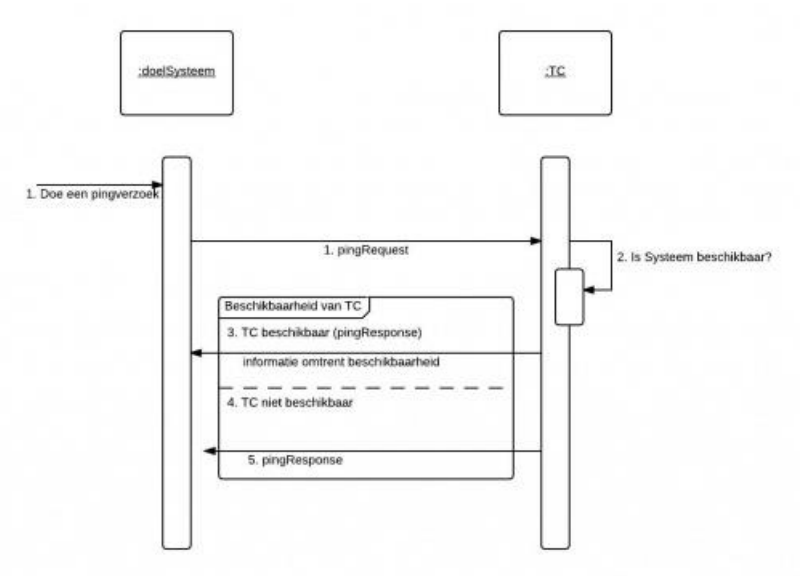
Het Traffic Center geeft een negatief antwoord terug omtrent de beschikbaarheid, het versienummer van de software welke op het Traffic Center draait en de huidige systeemtijd. Het Traffic Center is niet beschikbaar en/of de omgeving waar het Traffic Center op draait is niet beschikbaar. Er wordt geen antwoord teruggegeven aan het doelSysteem. Afhankelijk van de timeout instellingen bij het doelSysteem wordt er een timeout teruggegeven.

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

- Response:

```
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
   <SOAP-ENV:Header/>
   <SOAP-ENV:Body>
      <over:pingResponse xmlns:over="http://xml.eld.nl/schemas/Overstapservice/20140327">
         <over:available>true</over:available>
         <over:applicationVersion>2.1.9</over:applicationVersion>
         <over:systemTime>2014-09-29T04:05:37</over:systemTime>
      </over:pingResponse>
   </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

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).

APsleutel controleren

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.

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.)

*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 APsleutel bekend is in het Register
3. **If** APsleutel bekend
    1. **If** Leverancier (OIN uit certificaat) overeenkomt met geregistreerde Leverancier
        1. Het Traffic Center controleert of de waarden van BRIN en APindex voor het Aanleverpunt correct zin
        2. **If** waarden correct
            1. Traffic Center geeft bevestiging dat de APsleutel is gecontroleerd
        3. **Else**
            1. Traffic Center verstuurt foutmelding over BRIN/APindex aan Schoolsysteem
    2. **Else**
        1. Traffic Center verstuurt foutmelding over niet geautoriseerde Leverancier
4. **Else**
    1. Aanleverpunt verstuur foutmelding aan Schoolsysteem

Overzicht meldingen

Resultaat	**Type flow (N, A, E)**	**Omschrijving**
Aanleverpunt bij APsleutel correct	N	De validatie is succesvol
APsleutelOnbekend	E	De APsleutel komt niet voor in het Register.
OngeautoriseerdAanleverpunt	E	De Leverancier (op basis van de OIN uit het SAAS certificaat) komt niet overeen met waarden van het Aanleverpunt in het Register
AanleverPuntOnbekend	E	De opgegeven BRIN-APindex combinatie komt niet voor in het Register bij deze APsleutel

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

- 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.

Laten inzien dossier

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.

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:

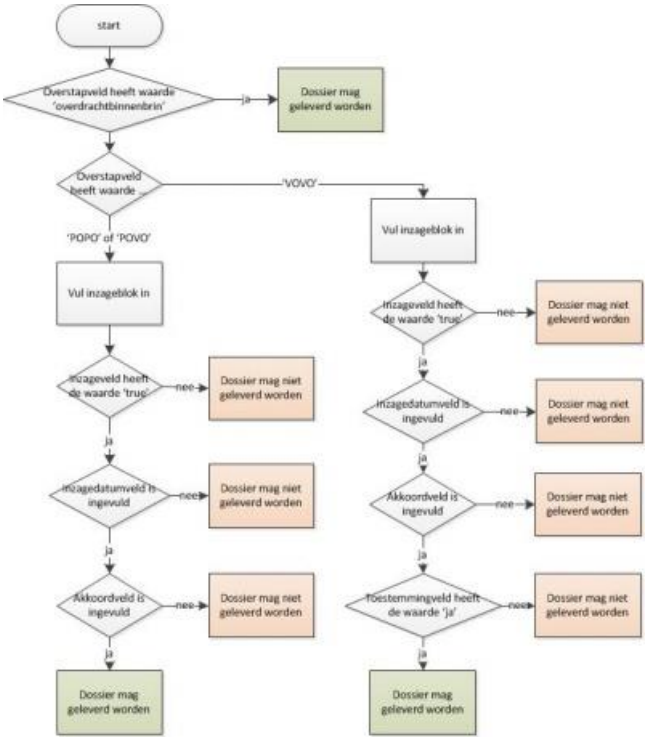
Type overstap	Eisen	Opmerkingen
PO-PO	Oudertoestemming is verplicht	
PO-VO	Ouderinzage is verplicht	
VO-VO	Oudertoestemming is verplicht	In het geval van een VOVO-uitwisseling dient de verzendende school voorafgaand aan de verzending te controleren of de ouders toestemming hebben gegeven voor het verzenden 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

Controleren formaat

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.

Gereed zetten 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

Klaarzetten dossier

Context

Voorafgaand aan de overdracht zet een Medewerker van een School een Dossier klaar. Bij het Klaarzetten wordt aangegeven welke Scholen een Dossier mogen ophalen (op BRIN(4) nivo). Een bronsysteem registreert deze Scholen bij het Dossier. Als een Dossier wordt opgevraagd door een Doelsysteem controleert het Bronsysteem of het Doelsysteem bij een School hoort waarvoor het Dossier is klaar gezet.

Onderliggende use cases

- Verwerken openstaande verzoeken (kleine notificatie) Medewerkers van een Bronschool kunnen op basis van een overzicht van binnengekomen verzoeken voor Dossiers deze aflopen en de betreffende dossiers gereed zetten.
- Gereed zetten dossier Het daadwerkelijk aangeven door een medewerker dat een Dossier gereed is voor verzending. Dit kan leiden tot het versturen van een of meerdere Notificaties.
    - Versturen notificatie Als een Dossier gereed wordt gezet dat eerder in aangevraagd maar niet uitgeleverd, kan een Notificatie verstuurd worden. Het versturen valt uiteen in twee stappen:
        - Notificatie melden Het melden van de Notificatie bij het Traffic Center en het ontvangen van de url van het Bronsysteem dat de Notificatie gaat ontvangen.
        - Notificatie versturen Het verzenden van de Notificatie naar het Doelsysteem.

Adressering

OSO eist dat een medewerker van Bronschool expliciet aangeeft welke Doelschool een Dossier mag ontvangen. Alleen wanneer het BRIN van de aanvragende school overeenkomt met deze waarde, mag het bronsysteem het dossier leveren.

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

Binnengekomen verzoeken

Een Bronsysteem moet de binnengekomen aanvragen van binnen het Bronsysteem bekende dossiers tonen aan eindgebruikers. De eindgebruikers kunnen deze lijst gebruiken om dossiers gereed te maken en klaar te zetten voor een OSO overdracht. Meer informatie

Versturen Notificatie

Als een Eindgebruiker in het Bronsysteem een Dossier Klaar zet, controleert het Bronsysteem of er voor dit specifieke Dossier verzoeken zijn binnengekomen. Als dat het geval is, moet er door het Bronsysteem een Notificatie naar het desbetreffende Doelsysteem worden verzonden. Meer informatie

- Gereed zetten dossier
    - Versturen notificatie
        - Notificatie melden
        - Notificatie versturen

Melden Notificatie

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

Preconditie

- BronSysteem is aangesloten op OSO keten
- BronSysteem heeft DocumentRequest ontvangen van Doelsysteem
- BronSysteem heeft Dossier klaargezet uit DocumentRequest van Doelsysteem

Postconditie

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

Basis scenario

1. Bronsysteem verstuurt Notificatie Melding naar Traffic Center
2. **If** het SessieID bekend is bij Taffic Center* **and** het DoelAanleverpunt heeft een URL geregistreerd
    1. Traffic Center registreert de Notificatie Melding
    2. **If** het DoelAanleverpunt is valide
        1. Traffic Center geeft url van het Bronaanleverpunt terug
    3. **Else**
        1. Traffic Center geeft foutmelding
3. **Else**
    1. Traffic Center geeft foutmelding

*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 orginele verzoek waar het sessieID aan werd toegekend.

Alternatieve scenario's:

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

Resultaat	A/E*	Omschrijving	Toelichting
AanmelderNietBekend	E	Bronsysteem (Aanleverpunt dat Notificatie meldt) is niet bekend bij het Traffic Center	In het Register is de combinatie van BronBRIN en APindex niet aanwezig.
AanvmelderNietCorrect	E	Bronsysteem (Aanleverpunt dat Notificatie meldt) is in het Register geregistreerd met andere Leverancier.	Het Aanleverpunt (BronBRIN/APindex) is bekend bij OSO, maar in het Register is een andere Leverancier bekend.
OntvangerNietBekend	E	Het opgegeven Aanleverpunt (DoelBRIN/APindex) van het Doelsysteem is niet bekend.	Het opgegeven Aanleverpunt van het Doelsysteem is (nog) niet opgenomen in het Register.
SessieIDNietBekend	A	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.
OntvangerNietBeschikbaar	A	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.
<Geen response>	E	Het Traffic Center geeft een time out of technische fout.	Het meldende Bronsysteem staakt de verdere Notificatie en geeft de eindgebruiker hierover een foutmelding.

* A: Alternatief, E: Exceptie (fout)

Aanroep en antwoord

- Request:

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
bronAPindex	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
doelAPindex	Dit is de index van het Aanleverpunt van het Doelsysteem dat de Sessie aanvraagt.	Verplicht
SessieID	De SessieID van het laatste documentRequest dat door het bronSysteem is ontvangen van het Doelsysteem	Verplicht
aanvraagDatum	Het tijdstip van het laatste documentRequest voor dit Dossier dat door het bronSysteem is ontvangen van het Doelsysteem	Verplicht

- Response

Versturen Notificatie

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

Preconditie

- BronSysteem is aangesloten op OSO keten
- BronSysteem heeft Notificatie melding verstuurd naar Traffic Center
- DoelSysteem is aangesloten op OSO keten
- DoelSysteem heeft documentRequest verstuurd naar Bronsysteem

Basis scenario

1. Bronsysteem verstuurt Notificatie naar Doelsysteem

Postconditie

- Doelsysteem heeft Notificatie ontvangen van Bronsysteem

Basis scenario

1. Bronsysteem verstuurt Notificatie naar Doelsysteem
2. Doelsysteem stuurt bevestiging ontvangst Notificatie aan BronSysteem*
3. Doelsysteem toont Notificatie gegevens aan Eindgebruiker (Doelsysteem)**
4. **If** Bronsysteem heeft bevestiging ontvangen
    1. BronSysteem toont bevestiging aan Eindgebruiker (Bronsysteem)
5. **Else**
    1. BronSysteem toont melding aan Eindgebruiker (Bronsysteem)***

*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 doelsysteem toont haar eindgebruiker informatie over het wel of niet succesvol versturen van de notificatie.

Aanroep en antwoord

- Request:

Element	Uitleg	Opmerkingen
bronBRIN	Dit is het BRINnummer van de Bronschool dat de Notificatie wil versturen.	
bronAPindex	Dit is de index van het Aanleverpunt van het Bronsysteem dat de Notificatie wil versturen.	
doelBrin	Dit is het brinnummer van het Doelsysteem dat de Notificatie ontvangt.	
bronAPindex	Dit is de index van het Aanleverpunt van het Doelsysteem dat de Notificatie ontvangt.	
BSN	Het BSN van het betreffende Dossier.	

- Response

Overdragen dossier

Context

De Overstapservice faciliteert het uitwisselen van gegevens (een ?document? of 'dossier' of 'OKR") tussen twee aangesloten systemen. Bij de daadwerkelijke uitwisseling van een dossier zijn drie systemen rechtstreeks betrokken:

1. Het informatiesysteem van de opvragende partij, het doelsysteem. Dit kan zowel een leerling administratie systeem (LAS) als een regionaal platform (RP) zijn.
2. Het informatiesysteem van de partij die gegevens kan aanleveren, het bronsysteem. Dit kan zowel een LAS als een RP zijn.
3. Het Traffic Center: Dit verzorgt primair de controle op de geldigheid van de uitwisselsessie tussen het doel- en bron- systeem en daarnaast heeft het een rol als register van de adressen van de systemen.

Berichten verkeer

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

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

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

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

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

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

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

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

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

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

Inzage en bewaartermijnen

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

Voor verzonden en ontvangen dossiers geldt een bewaartermijn.

Organisatorische randvoorwaarden

Het te verzenden Dossier moet voldoen aan de eisen gesteld vanuit de Edukoppeling OSO dossier specificatie. OSO volgt versie 2016.1. Voorafgaan aan verzending dient het dossier gevalideerd te worden op:

- het dossier dient qua ?vorm? te voldoen aan de specificatie gevalideerd tegen de xsd
- de inhoud van het dossier

Deze validatie kan door het Bronsysteem zelf worden uitgevoerd of door het KVS.

Verschillende overdrachten

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

Overdrachtsoort

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

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

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

Initiëren sessie

Actor(s)	Goal(s)
Systeem (doelschool)	Geldige sessie toegekend krijgen voor opvragen specifiek dossier
Traffic Center	Sessie toekennen aan systeem voor geldig verzoek van systeem voor specifiek dossier door school

Preconditie

Systeem (doelBrin) is toegelaten op OSO keten

Postconditie

Systeem (doelBrin) heeft sessie toegekend gekregen voor opvragen specifiek dossier bij aangeduide systemen

Basis scenario

1. Doelsysteem vraagt sessie aan bij het Traffic Center voor opvragen specifiek dossier(BSN) bij specifieke Bronschool
2. **If** het Doelsysteem is valide **And** Bronschool heeft geregistreerde Aanleverpunten **then**
    1. Traffic Center kent een sessie toe aan het Bronsysteem
    2. Traffic Center verstrekt lijst met te bevragen Aanleverpunten
    3. DoelSysteem gaat naar Dossier opvragen
3. **Else**
    1. Traffic Center geeft foutmelding terug
    2. Doelsysteem geeft foutmelding aan Eindgebruiker *

*In dit geval kan de Sessie niet afgemeld worden.

Variant: Specifieke opvraag

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 valide).

Alternatieve scenario's:

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

Resultaat	A/E*	Omschrijving	Toelichting
AanvragerNietBekend	A	Doelsysteem (aanvragend aanleverpunt) is niet bekend bij het Traffic Center	In het Register is de combinatie van DoelBRIN en APindex niet aanwezig.
AanvragerNietBeschikbaar	A	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.
AanvragerNietCorrect	A	Doelsysteem (aanvragend AP) is in het Register geregistreerd met andere Leverancier.	Het Aanleverpunt (BronBRIN/APindex) is bekend bij OSO, maar in het Register is een andere Leverancier bekend dat die deze sessie aanvraag indient.
VerstrekkerNietBekend	A	Bronbrin is niet bekend bij het Traffic Center.	De opgegeven Bronschool is (nog) niet opgenomen in het Register.
VerstrekkerNietBeschikbaar	A	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.
GeenRelatieMetDoel	A	De overdrachtSoort in het overdrachtsRequest is "overdrachtbinnenbrin", maar het bronBRIN en doelBRIN verschillen van elkaar.	Een 'binnenBRIN' overdracht mag alleen tussen systemen met eenzelfde BRIN plaats vinden.
OverdrachtReedsActief	E	Er is reeds een sessie actief voor dezelfde parameters.	Een sessie voor een identieke overdracht is nog actief.
<Geen response>	E	Het Traffic Center geeft een time out of technische fout.	Het aanvragende Bronsysteem staakt de verdere aanvraag en geeft de eindgebruiker hierover een foutmelding.

* A: Alternatief, E: Exceptie (fout)

Aanroep en antwoord

- Request:

Element	Uitleg	Opmerkingen
bronBRIN	Dit is het brinnummer van de Bronschool waar dossier van specifieke leerling wordt opgevraagd.	De Bronschool kan meerdere Aanleverpunten hebben.
bronAPindex	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.	
doelAPindex	Dit is de index van het Aanleverpunt van het Doelsysteem dat de Sessie aanvraagt.	
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

Opvragen dossier

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

Preconditie

Dossier is klaargezet door schoolmedewerker (bronschool) voor doelschool Geldige sessie voor opvragen dossier is toegekend aan Doelsysteem

Postconditie

Dossier is verzonden van Doelsysteem naar Bronsysteem

Basis Scenario

1. Doelsysteem vraag dossier op [#]
2. Bronsysteem laat Sessie gegevens Controleren bij TC[*]
3. **If** sessie gegevens valide blijken
    1. *Bronsysteem slaat aanvraag gegevens (bsn, sessie id, documentRequest, doel brin, doel ap index, aanvraagDatum) 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**
        1. Bronsysteem verstuurt foutmelding

[#] In OSO'16 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. [**]Het Dossier is klaargezet en (indien van toepassing) inzage heeft plaats gevonden
[***]Bij het Dossier is door de Eindgebruiker (Bronsysteem) aangegeven dat het opgevraagd mag worden door de School (BRIN).
[****]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 ?datum aanvraag? 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).
- Als de parameter niet is ingevuld, volgt de ?normale? afhandeling van het request.

Aanpassing tov OSO'15

Scenario's

Rangorde*	Resultaat	Type flow (N, A, E**)	Omschrijving	Stopcriterium bij aflopen aanleverpunten
0	<Document>	N	Het gevraagde document. (Let op: In het afmeldingRequest moet dan status='VerstrekkingGeslaagd' worden gebruikt)	nee
1	LeveringInBehandeling***	A	Het leverende systeem (bron) kan niet bepalen of het dossier beschikbaar is of dat de leerling bij bij de bron bekend is. Deze melding is geen stopcriterium, dus het aanvragende systeem (doel) gaat hierna verder met het doorlopen van de andere aanleverpunten.	nee
2	LeerlingInfoNietGewijzigd	A	De inhoud van het Dossier is sinds de opgegeven 'aanvraagdatum? in het documentRequest niet gewijzigd.	ja
2	DossierVersieNietCorrect*****	A	De versie van het Dossier dat klaar staat wijkt af van de huidige versie (en kan daardoor niet correct geïmporteerd worden).	ja
3	LeerlinginfoNietOpvraagbaar	A	Het Dossier mag niet worden verstrekt, omdat de ouders/leerling geen toestemming hebben verleend.	ja
4	LeerlinginfoNietIngezien****	A	Het document mag (nog) niet worden verstrekt, omdat de ouders nog geen inzage hebben gehad.	ja
5	LeerlinginfoNietBeschikbaar	A	Het Dossier is (nog) niet klaargezet voor overdracht.	ja
6	LeveringGeweigerd	A	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
7	LeerlingNietBekend	A	De leerling met het opgegeven BSN is niet bekend bij het leverende bronsysteem.	nee
8	AuthenticatieVerstrekkerMislukt	E	Het leverende bronsysteem kon zich niet authenticeren bij het Traffic Center. Het opvragende doelsysteem hoeft hierop geen actie te ondernemen.	nee
9	SessieOngeldig	E	De sessie is ongeldig; het sessie-ID is nooit uitgedeeld. Dit is het resultaat van de sessieControle.	nee
10	SessieAfwijkend	E	De overstapvraag wijkt af van die, waarmee de sessie verkregen is. Dit is het resultaat van de sessieControle.	nee
11	SessieReedsAfgemeld	E	De sessie is al afgemeld en dus niet langer geldig. Dit is het resultaat van de sessieControle.	nee
12	SessieVerlopen	E	De sessie is verlopen; de time-out is verstreken. Dit is het resultaat van de sessieControle.	nee
13	Communicatiefout	E	Het leverende bronsysteem geeft geen antwoord of er treedt een (technische) fout op. Er is geen contact geweest met het leverende bronsysteem.	nee

[*] 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.
[**] N: Normaal, A: Alternatief, E: Exceptie (fout)
[***]Deze melding is optioneel, niet alle systemen kennen deze toestand.
[****]POVO overstap.
[*****]Nieuw in OSO'16.

Aanroep en antwoord

- Aanroep:

Element	Uitleg	Opmerkingen
bronBrin	Dit is het BRIN van de bronschool.	
bronAPindex	Dit is de index van het aanleverpunt van het bronsysteem dat dit verzoek ontvangt.	
doelBrin	Dit is het BRIN van de doelschool	
doelAPindex	Dit is de index van het Aanleverpunt van het Bronsysteem dat dit verzoek indient.	
zoeksleutel	Dit is de versleutelde BSN	Dit moet exact overeenkomen met de zoeksleutel zoals meegegeven bij het aanvragen van een sessie
overdrachtsoort	Dit bepaalt om wat voor soort overdracht het gaat, een overstapdossier of overdrachtbinnenbrin.	De overdrachtsoort wordt overeenkomen met de overdrachtsoort welke gebruikt is in het overdrachtsRequest. Het BRIN-nummer van het bron- en doelBRIN moet hetzelfde zijn voor een binnenbrin overdracht.
sessieId	De sessie-ID die verkregen is bij het Initiëren van de Sessie.	
BSN	Het BSN van de leerling	Dit wordt onversleuteld verstuurd in het documentRequest

- Antwoord:

Sessie controleren

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

- Doelsysteem heeft een geldige sessie aangevraagd en toegekend gekregen
- Bronsysteem heeft een verzoek voor een specifiek dossier van Systeem (doelschool) ontvangen

Postconditie

- Traffic Center heeft vastgesteld of gegevens uit verzoek voor dossier overeenkomen met gegevens uit toegekende sessie.

Basic Path

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

Aanroep en antwoord

- Request:

- Response

Element	Uitleg	Opmerkingen
bronBRIN	Dit is het brinnummer van de Bronschool waar dossier van specifieke leerling wordt opgevraagd.	De Bronschool kan meerdere Aanleverpunten hebben.
bronAPindex	Dit is de index van het Aanleverpunt van het Bronsysteem dat bevraagd wordt (optioneel).	Deze parameter kan meegegeven worden wanneer het Doelsysteem één specifiek Aanleverpunt van de School wil bevragen.
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.	
bronAPindex	Dit is de index van het Aanleverpunt van het Doelsysteem dat de Sessie aanvraagt.	
zoeksleutel	De zoeksleutel wordt overgenomen vanuit het documentsRequest.	
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.
aanleverpunt	Het aanleverpunt van het Systeem (bronschool)	
sessieId		

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?.

Meervoudige ontvangst

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

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

Sessie afmelden

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 <LINK> dat binnen de sessie teruggegeven is door een bevraagd Aanleverpunt.

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)

Aanroep en antwoord

- Aanroep:
- Antwoord:

sessieid, status ('beste resultaat') :-)

Element	Uitleg	Opmerkingen
bronBRIN	Dit is het brinnummer van het Bronsysteem. Het TC controleert of het Bronsysteem bekend en actief is in het deelnemersregister.	
bronAPindex	Dit is de index van het Aanleverpunt van het Bronsysteem.	
doelBrin	Dit is het brinnummer van het Doelsysteem. Het TC controleert of het Doelsysteem bekend en actief is in het deelnemersregister.	
doelAPindex	Dit is de index van het Aanleverpunt van het Doelsysteem.	

Beveiliging

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 LAS systemen in hun interactie met het TS

Aangesloten Systemen

Leerling Administratie Systemen (LAS) 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 het burgerservicenummer (BSN) gebruikt. Daar heet het persoonsgebonden nummer (PGN), maar het gaat om hetzelfde nummer. In sommige gevallen hebben leerlingen (nog) geen BSN of sofinummer, bijvoorbeeld asielzoekers of leerlingen die niet in Nederland wonen. In dit geval krijgen ze een tijdelijk onderwijsnummer.

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.

prefix	Betekenis
2318	Gebruik dit prefix voor een PGN van type BSN
3872	Gebruik dit prefix voor een PGN van type tijdelijk onderwijsnummer

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>0EVKqqr5JyI4tYnOO1sDbazqyJY78rpBcvrcmbimjRkcwkpQ1knwVKURccH5oaSdhaXptg+9QcBqbC0p3SLy
m7f3hyeLCJvxNEV4JPZ7L5GbnsC8Ux5HxLinW/B6mF8jMYh5du5X7OKytNA2qlGdwe7qM</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/20140327">
   <soapenv:Header/>
   <soapenv:Body>
    <ns:overdrachtRequest>
      <ns:overdracht>
        <ns:bronBrin>98PO</ns:bronBrin>
        <ns:doelBrin>98VO</ns:doelBrin>
        <ns:zoeksleutel>534534efgrt34563ery345345eferert34345</ns:zoeksleutel>
        <ns:overdrachtsoort>overstapdossier</ns:overdrachtsoort>
      </ns:overdracht>
    </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.

```
openssl genrsa -des3 -out private.pem 4096
```

Hetzelfde, maar dan zonder wachtwoord

```
openssl genrsa -out private.pem 2048
```

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 op korte termijn 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

Verklaring

Een certificaat keten bestaat uit het webserver 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 dat bij de client.

client certificaten

Vanaf OSO'16 wordt 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).

Het voorstel om te komen tot de wijzigingen in het gebruik van certificaten is terug te lezen in dit memo: Bestand:Memo Voorstel wijzigen PKI infrastructuur.pdf.
Een lijst met vragen over de wijziging in de PKI infrastructuur met antwoorden wordt OSO:2016/beveiliging/FAQ hier bijgehouden.

Leverancier van certificaten

Eisen

- Het client certificaat **moet** uitgegeven worden door een gekwalificeerd uitgever van "Staat der Nederlanden" certificaten.
- Het client certificaat **moet** ondertekend zijn door "Staat der Nederlanden Autonome Apparaten CA - G2" **of** "Staat der Nederlanden Autonome Apparaten CA - G3"
- 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 Autonome Apparaten", zoals na te lezen op de site van Logius. Het CA certificaat waartegen OSO valideert is het intermediate certificaat "Staat der Nederlanden Autonome Apparaten CA - G2" en "Staat der Nederlanden Autonome Apparaten CA - G3". 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.

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.

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. **TODO: Procedure aanvragen Sandbox certificaat toevoegen**

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 online via het certificaat register dat t.z.t. online verschijnt. **TODO: Register publiceren**

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.

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. 0x13 ECDHE-RSA-AES128-SHA
5. 0x28 ECDHE-RSA-AES256-SHA384
6. 0x14 ECDHE-RSA-AES256-SHA

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

1. 0x2B ECDHE-ECDSA-AES128-GCM-SHA256
2. 0x2C ECDHE-ECDSA-AES256-GCM-SHA384
3. 0x23 ECDHE-ECDSA-AES128-SHA256
4. 0x09 ECDHE-ECDSA-AES128-SHA
5. 0x24 ECDHE-ECDSA-AES128-SHA256
6. 0x0A ECDHE-ECDSA-AES256-SHA

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. 0x33 DHE-RSA-AES128-SHA
4. 0x6B DHE-RSA-AES256-SHA256
5. 0x39 DHE-RSA-AES256-SHA

Opmerkingen bij DHE:

- **Vereist** zelf gegenereerde DH parameters
- **Vereist** DH sleutel lengte van tenminste 2048bit (gelijk aan RSA privé sleutel)

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

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.

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.

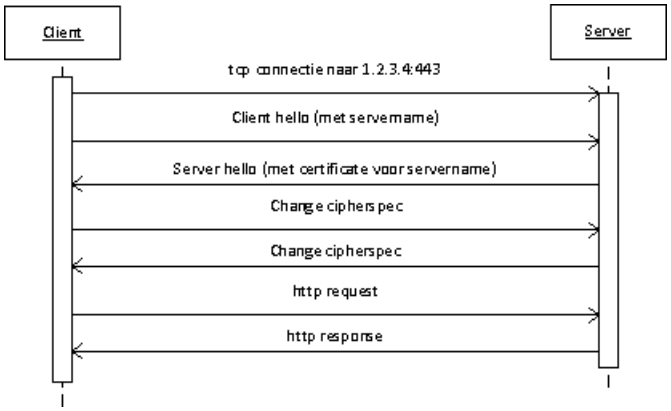
ServerNameIndication

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

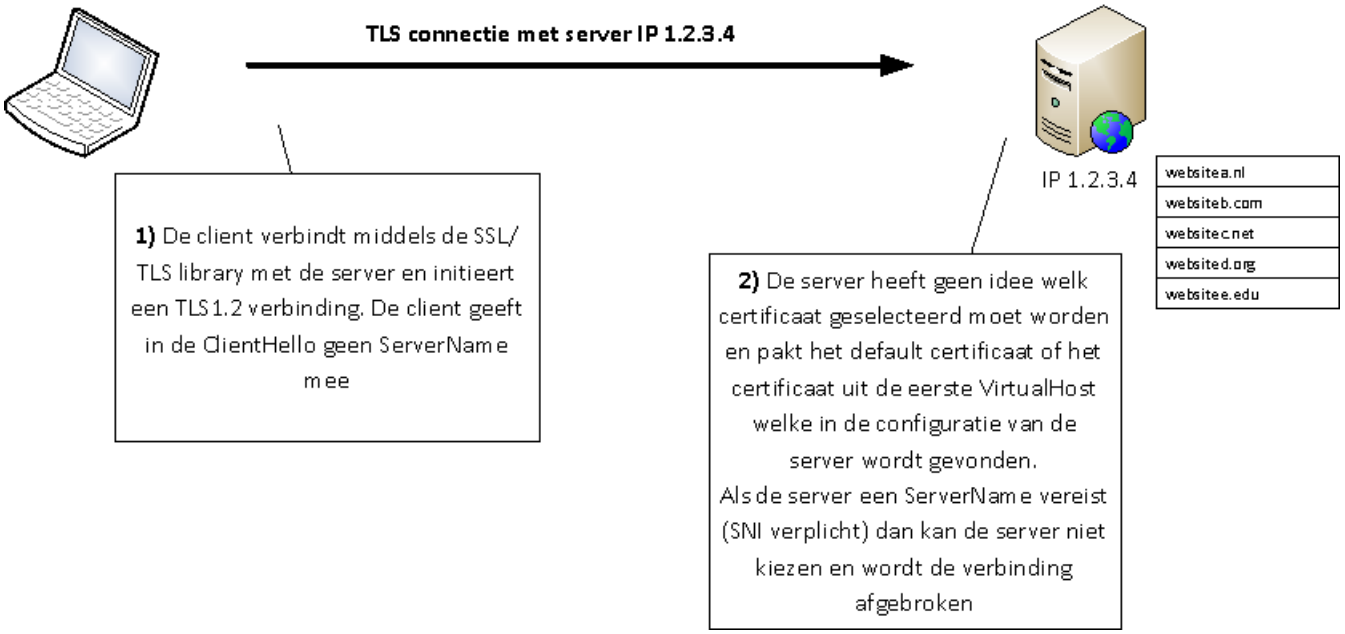
Verklaring

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.

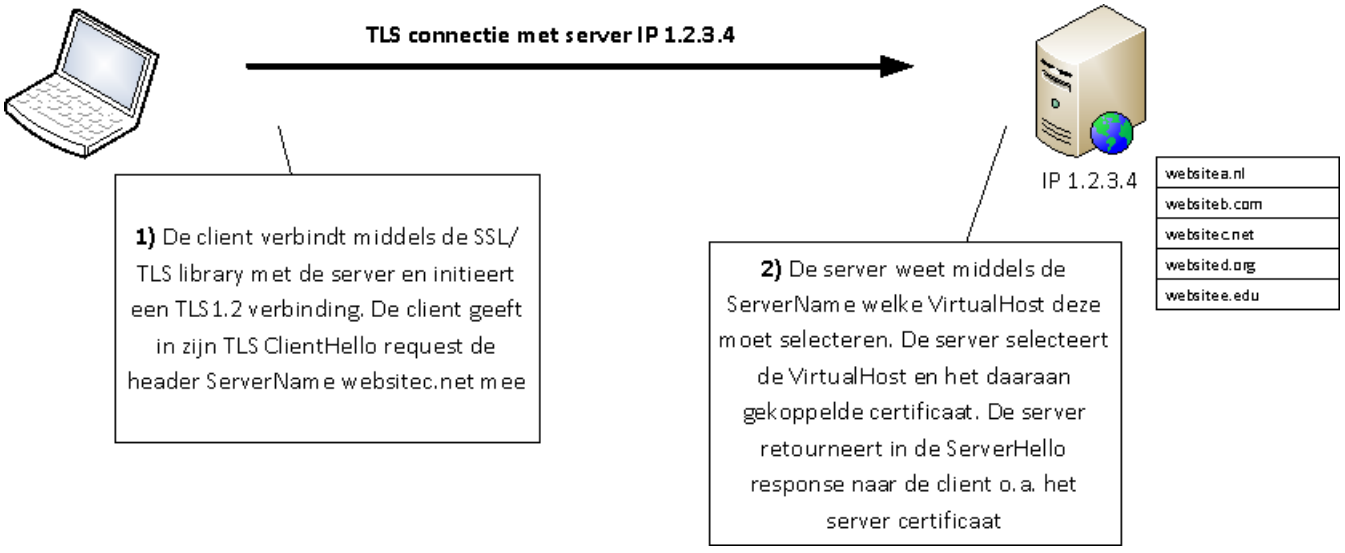


Dit ziet er als hiernaast uit:
Elke client moet dit binnen OSO ondersteunen omdat er reeds leveranciers zijn die server-side SNI nodig hebben om het juiste certificaat te kunnen retourneren aan de client.
Ter illustratie schematisch weergegeven hoe de communicatiestroom er met en zonder SNI uitziet:

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

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 is nog experimenteel en niet breed ondersteund. Het zal in de toekomst mogelijk wel een eis gaan worden.

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	• Doelsysteem verifieert het servercertificaat van Bronsysteem. • Bronsysteem verifieert het clientcertificaat van het Doelsysteem. • 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.

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 gekwalificeerde 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