OSR kwalificatie testplan 2019

versie 1.0
21 februari 2019

Wijzigingen voor 0.1 (12-01-2019)
- Initiële opzet document
Wijzigingen voor 0.2 (06-02-2019)
- Aanvullingen REST calls
Wijzigingen voor 1.0 (21-02-2019)
- Opmerkingen verwerkt

Inhoudsopgave

1 Inleiding

Dit document beschrijft de functionele en inhoudelijk testen van VO lassen die OSR berichten gaan uitwisselen met het Onderwijsserviceregister.
De systemen die getest worden moeten voldoen aan eisen opgenomen in de OSR developers wiki.

1.1 Testomgeving

De test vindt plaats op de Qualification-omgeving.
Op de Qualification-omgeving amoeten de leveranciers het PKIoverheid-certificaat gebruiken.
Voor de volledigheid: de beveiligingstest zal op de productieomgevingen plaatsvinden.

1.2 Basis voor het testplan

De volgende documenten vormen de basis voor dit testplan.

Document omschrijving	Versie	Datum	Documentnaam/locatie
OSR wiki	n.v.t.		https://developers.wiki.kennisnet.nl/index.php?title=OSR:Hoofdpagina
Edukoppeling REST ondertekening (JWT)	0.2	20-12-2018	https://docs.google.com/document/d/1YsLjjcaAKFWb8dxUvk-89ttt8kCgX3kAuLtZPY5uAgU/edit#heading=h.7dn462l5hmxs
OSR REST		2019	https://osr-api-sb.kennisnet.nl/api/v1/doc (te benaderen met een self signed test certificaat)

2 Testscenario’s LAS VO/VAVO -> OSR

2.1 Controleren of een school een mandaat heeft afgegeven voor je LAS

Indien een LAS diensten namens een school wilt gaan leveren, moet deze school eerst een mandaat hebben afgegeven.

Ergens in de flow van de LAS moet een check worden gebouwd met deze controle. Als de check faalt, dient de LAS een foutmelding aan te gebruiker te tonen.

De mandaat check heeft als parameter OIN van een school nodig. Dus deze moet als eerst worden opgehaald.

2.1.1 Normal flow: Ophalen OIN school op basis van BRIN4

	Wie	**Actie**
1.	LAS	Het LAS haalt het oin op van school 00AB. Technisch: Het LAS verstuurt een REST API call: **/api/v1/schools?brin=00AB** naar het OSR. 00AB moet worden vervangen met BRIN4 van de op te vragen school. Zie ook de developers wiki. “Opvragen informatie onderwijsinstelling”
2.	OSR	OSR geeft een antwoord met o.a. het OIN van de school.

2.1.2 Exceptional flow: Ophalen OIN school op basis van BRIN4 (Brin bestaat niet)

	Wie	**Actie**
1.	OSR	Beheerder van OSR verandert de BRIN in de OSR database, waardoor deze niet meer op te vragen is.
2.	LAS	Het LAS verstuurt een REST API call: **/api/v1/schools?brin=00AB** naar het OSR. 00AB moet worden vervangen met BRIN4 van de op te vragen school.
3.	OSR	OSR geeft een leeg antwoord terug: [ ].
4.	LAS	Toont de melding dat er een fout is opgetreden en logt de fout.

2.1.3 Normal flow: Mandaat ophalen

	Wie	**Actie**
1.	LAS	Het LAS verstuurt een **/api/v1/mandates** API call naar het OSR met de volgende parameters: OIN LAS (uit het SSL certificaat), OIN school, namespace van de dienstversie (bv. http://xml.eld.nl/schemas/VVA/20190221)

2.	OSR	OSR antwoordt met een lijst van endpoints met o.a. een token die gebruikt kan worden om een endpoint aan te maken.

2.1.4 Normale flow: Mandaat ophalen (leeg resultaat)

Een mandaat wordt opgehaald door LAS, maar OSR geeft een leeg resultaat terug. Dit kan ook gebeuren indien een mandaat van een andere LAS opgehaald wordt.

	Wie	**Actie**
1.	OSR	OSR beheerder verandert binnen de OSR database het OIN dat bij een leverancier hoort. Het mandaat bestaat dus, maar LAS is niet de eigenaar.
2.	LAS	Het LAS verstuurt een **/api/v1/mandates** API call naar het OSR met de volgende parameters: OIN van een andere LAS, OIN school, namespace van de dienstversie (bv. http://xml.eld.nl/schemas/VVA/20190221)
3.	OSR	OSR antwoordt met een lege string (response 200 OK). Dat wil zeggen dat het mandaat wel bestaat, maar de opvrager is niet de eigendaar ervan.
4.	LAS	Toont de melding dat er een fout is opgetreden en logt de fout.

2.1.5 Normale flow: Mandaat ophalen (tijdrijzen)

Een mandaat wordt opgehaald door LAS dat verlopen of nog niet geldig is, maar omdat reference_date wordt meegegeven krijg je toch een resultaat.

	Wie	**Actie**
1.	OSR	OSR beheerder verandert binnen de OSR database de einddatum van een mandaat dat bij een leverancier hoort, waardoor het mogelijk wordt om een mandaat in het verleden of in de toekomst op te vragen.
2.	LAS	Het LAS verstuurt een **/api/v1/mandates** API call naar het OSR met de volgende parameters: OIN LAS (uit het SSL certificaat), OIN school, reference_date (in het verleden of toekomst), namespace van de dienstversie (bv. http://xml.eld.nl/schemas/VVA/20190221)
3.	OSR	OSR antwoordt met een lijst van endpoints met o.a. een token

2.1.6 Exceptional flow: Mandaat ophalen (404: Mandate not found)

Een mandaat wordt opgehaald door LAS, maar OSR geeft een leeg resultaat terug

	Wie	**Actie**
1.	OSR	OSR beheerder verandert binnen de OSR database het mandaat zodat het mandaat niet lijkt te bestaan. Bv. de gebruikte namespace version wordt veranderd.

2.	LAS	Het LAS verstuurt een **/api/v1/mandates** API call naar het OSR met de volgende parameters: OIN LAS (uit het SSL certificaat), OIN school, namespace van de dienstversie (bv. http://xml.eld.nl/schemas/VVA/20190221)
3.	OSR	OSR antwoordt met een 404: mandate not found foutmelding. Dat wil zeggen dat het mandaat niet bestaat.
4.	LAS	Toont de melding dat er een fout is opgetreden en logt de fout.

2.2 Endpoints

Als een school een mandaat aan een LAS heeft afgegeven kan een leverancier endpoints aanmaken en bewerken voor deze school.

2.2.1 Normal flow: (Optioneel) Endpoints ophalen

Elke leverancier heeft per dienstversie een URL gedefinieerd. Deze worden in OSR bewaart. Het kan voorkomen dat een leverancier zijn eigen endpoints (of die van een andere school) wil ophalen.

	Wie	**Actie**
1.	LAS	Het LAS verstuurt een **/api/v1/endpoints** API call naar het OSR met de volgende parameters: Namespace van de dienstversie (bv. http://xml.eld.nl/schemas/VVA/20190221), School OIN of Administration ID.
2.	OSR	OSR antwoordt met een lijst van endpoints, die zijn opgeslagen binnen OSR.
3.	LAS	LAS controleert of zijn endpoints nog kloppen.

2.2.2 Exceptional flow: Opgevraagde endpoint niet meer beschikbaar

Het kan voorkomen dat een endpoint niet meer beschikbaar is, het systeem moet dat herkennen en een melding aan de gebruiker tonen.

	Wie	**Actie**
1.	OSR	OSR beheerder verandert binnen de OSR database de endpoints zodat ze niet lijkten te bestaan. Bv. Einddatum wordt naar een datum in het verleden aangepast.
2.	LAS	Het LAS verstuurt een **/api/v1/endpoints** API call naar het OSR met de volgende parameters: Namespace van de dienstversie (bv. http://xml.eld.nl/schemas/VVA/20190221), School OIN of Administration ID.
3.	OSR	OSR antwoordt met een lege lijst van endpoints. (Lege array [])
4.	LAS	LAS controleert of zijn endpoints nog kloppen.

2.2.3 Normal flow: Endpoint aanmaken

	Wie	Actie
1.	LAS	Het LAS verstuurt een **/api/v1/endpoints** (POST) API call naar het OSR om een endpoint aan te maken en gebruikt hiervoor de volgende parameters: Eerder verkregen mandaat token, namespace van de dienstversie (bv. http://xml.eld.nl/schemas/VVA/20190221), Administratie ID. De header moet ook een geldig JWT token bevatten.

2.	OSR	OSR antwoordt dat het endpoint is aangemaakt.
		
		Bv.
		{
		"attributes": "Test",
		"administration_id": "00000007000000000013",
		"url": "https://valide-url.nl",
		"start_date": "2019-01-23",
		"end_date": null,
		"_links": {
		"self": {"href": "/api/v1/endpoints/20"},
		"school": {"href": "/api/v1/schools/1"},
		"service": {"href": "/api/v1/services/2"},
		"service-version": {"href": "/api/v1/service-versions/1"}
		}
		}

3.	LAS	Toont een melding op scherm dat het endpoint is aangemaakt en schrijft dat weg is eigen log.

2.2.4 Exceptional flow: 403 (not qualified) Endpoint aanmaken mislukt

	Wie	Actie
1.	OSR	OSR beheerder verandert binnen de OSR database zodat het lijkt dat de leverancier niet meer gekwalificeerd is
2.	LAS	Het LAS verstuurt een **/api/v1/endpoints** (POST) API call naar het OSR om een endpoint aan te maken en gebruikt hiervoor de volgende parameters: Eerder verkregen mandaat token, namespace versie van de dienst (bv. http://xml.eld.nl/schemas/VVA/20190221), Administratie ID. De header moet ook een geldige JWT token bevatten.

3.	OSR	OSR antwoordt met de foutmelding:
		
		{
		"code": 403,
		"message": "You are not qualified to create an endpoint."
		}

4.	LAS	Toont een melding aan de gebruiker dat het endpoint is niet aangemaakt en schrijft dat weg is eigen log.

2.2.5 Exceptional flow: 403 (mandaat verlopen) Endpoint aanmaken mislukt

	Wie	Actie
1.	OSR	OSR beheerder verandert binnen de OSR database het mandaat zodat deze verlopen is. Bv. een mandaat is geldig van start_date: 2019-01-01 t/m end_date: 2019-02-14.
2.	LAS	Het LAS verstuurt een **/api/v1/endpoints** (POST) API call naar het OSR om een endpoint aan te maken en gebruikt hiervoor de volgende parameters: Eerder verkregen mandaat token, namespace versie van de dienst (bv. http://xml.eld.nl/schemas/VVA/20190221), start_date: 2018-12-31 Administratie ID. De header moet ook een geldige JWT token bevatten.

3.	OSR	Let op. OSR antwoord voor het aanmaken of bewerken van een endpoint is een array. Er kunnen dus meerdere fouten worden teruggegeven. bv:
		
		[
		{
		"parameter": "start_date",
		"value": "2018-12-31",
		"message": "This value needs to be a date after or equal with the start date of the mandate used (2019-01-01)."
		},
		{
		"parameter": "start_date",
		"value": "2018-12-31",
		"message": "This value needs to be a date after or equal to today (2019-02-19)."
		}
		]

4.	LAS	Toont een melding aan de gebruiker dat het endpoint is niet aangemaakt en schrijft dat weg is eigen log.

2.2.6 Exceptional flow: 403 (administratiekermerk bestaat al) Endpoint aanmaken mislukt

	Wie	Actie
1.	LAS	Het LAS verstuurt een **/api/v1/endpoints** (POST) API call naar het OSR om een endpoint aan te maken en gebruikt hiervoor de volgende parameters: Eerder verkregen mandaat token, namespace versie van de dienst (bv. http://xml.eld.nl/schemas/VVA/20190221), Administratie ID die al eerder gebruikt is om een endpoint aan te maken. De header moet ook een geldige JWT token bevatten.

2.	OSR	OSR antwoordt met de foutmelding:
		
		[
		{
		"message": "An endpoint already exists for service version with namespace http:\/\/vokoppelpunt.vroegtijdigaanmelden.nl\/v1_0\/ and administration id 00000007000000000013."
		}
		]

3.	LAS	Toont een melding aan de gebruiker dat het endpoint is niet aangemaakt en schrijft dat weg is eigen log.

2.2.7 Optioneel: Endpoint aanmaken (JWT token response controleren)

	Wie	Actie
1.	LAS	Het LAS verstuurt een **/api/v1/endpoints** (POST) API call naar het OSR om een endpoint aan te maken of te bewerken. Het is niet nodig om geldige parameters or een geldige JWT token mee te sturen

2.	OSR	OSR geeft een antwoord met in de header een JWT token. De issuer in de payload bevat het OIN van Kennisnet en de audience is het OIN van de leverancier die de aanvraag gedaan heeft. Deze waarden zijn omgedraaid in de request.
		
		{
		"iat": 1550588400,
		"nbf": 1550588400,
		"exp": 1550592000,
		"aud": "00000003272448340204",
		"iss": "00000003272448340116",
		"edustd:body": {
		"alg": "B64SHA256",
		"hash": "DmSGW0lCV3OSNp/rVgGpodZ/Hcuje5ciQkiDqPhFpAk="
		}

3.	LAS	Het is aan het LAS om de JWT token op correctheid te controleren en een foutmelding te tonen op het moment als er een fout optreedt.

2.2.8 Normal flow: Endpoint aanpassen

	Wie	Actie
1.	LAS	Het LAS verstuurt een **/api/v1/endpoints/{id}** (PUT) API call naar het OSR om een endpoint aan te passen en gebruikt hiervoor het {id} dat binnen OSR is opgeslagen: Eerder opgehaalde mandaat token, namespace van de dienstversie (bv. http://xml.eld.nl/schemas/VVA/20190221), Administratie ID. De header moet een geldig JWT token bevatten.
2.	OSR	OSR antwoordt dat het endpoint is aangepast.
3.	LAS	Toont een melding aan de gebruiker dat het endpoint is aangepast en schrijft dat weg is eigen log.

3 Eisen aan logging

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

- het kunnen achterhalen welk bericht 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)

	Wie	**Actie**
1.	LAS	Controleer of het volgende gelogd wordt: - Tijdstip request - Request method - Request URI - Request Parameters - JWT token - Tijdstip response - Response content - Response Status - Gebruiker ID van het systeem
2.	LAS	De informatie in een logregel voor de gebruiker is voldoende zelf beschrijvend om zonder contextinformatie uit het bronsysteem de actie te kunnen herleiden tot de verantwoordelijke (rechts)persoon.
3.	LAS	Een systeem registreert logregels voorzien van datum en tijd, met een nauwkeurigheid van ten minste 1 seconde.
4.	LAS	Een systeem garandeert een maximale afwijking van de UTC + 01:00 tijd (de tijdzone waarin Nederland valt) van 5 seconden.
5.	LAS	Logregels voor de gebruiker kunnen na creatie niet worden aangepast of verwijderd.

4 Beveiliging

4.1 Certificaat validatie

Leveranciers moeten controleren op certificaten bij binnenkomende verzoeken.

De request worden gedaan met 2 verschillende certificaten:
- Self-signed certificaat, welke niet uitgegeven is door een legitieme CA.
- PKI-overheidscertificaat welke valide is en geaccepteerd moet worden

De leverancier moet het self-signed certificaat request afkeuren en alleen de requests met een PKI-overheidscertificaat toelaten.
In de praktijk is gebleken dat leveranciers een afwijkende response teruggeven. Er dient een HTTP 403 error teruggegeven worden indien een cliënt met een niet valide certificaat een request verstuurd.

De algemene beveiligingseisen zijn opgenomen in de developers wiki:

https://developers.wiki.kennisnet.nl/index.php?title=Standaarden:Beveiligd_Gegevenstransport