# Intakeadvies OAS versie 3.1

| | |
|---|---|
| Vergadering: | Forum Standaardisatie 7 december 2022 |
| Agendapunt: | 3B |
| Documentnummer: | FS-20221207.3B-Intakeadvies-Versiewijziging-OAS |
| Aan: | Forum Standaardisatie |
| Van: | Stuurgroep Open Standaarden |
| Datum: | 17 november 2022 |
| Versie: | 1.0 |
| Bijlagen: | geen |
| Rechten: | CC0 publieke domein verklaring |

## 1 Samenvatting en advies

De Stuurgroep Open Standaarden adviseert het Forum Standaardisatie om te toetsen of de standaard OpenAPI Specification (OAS) in de nieuwe versie (3.1) geschikt is om te blijven verplichten aan de overheid ('pas toe of leg uit'-verplichting). Een volledig expertonderzoek is aangewezen om de nieuwe versie van de standaard te toetsen aan de criteria voor opname op de lijst. OAS is een standaard voor het beschrijven van REST API's.

De indiener Logius verzoekt om de versie van OAS te actualiseren op de 'pas toe of leg uit'-lijst vanuit het belang dat OAS wordt gebruikt in andere standaarden van Logius, waaronder Digikoppeling (in het bijzonder koppelvlakspecificatie REST-API). De huidige versie 3.0 op de 'pas toe of leg uit'-lijst is niet de gangbare versie. OAS is een internationale standaard met een internationale beheerorganisatie (OpenAPI Initiative). OAS 3.0 staat sinds 2018 op de 'pas toe of leg uit'-lijst na aanmelding door Het Kadaster. In Nederland is er geen organisatie die de regierol voert over het Nederlandse beheer of stimuleren van adoptie van OAS.

Tijdens het intakegesprek zijn de diverse criteria besproken. OAS in de nieuwe versie (3.1) lijkt kansrijk om te blijven verplichten aan de overheid. Tijdens de expertbijeenkomst en het tot stand komen van het expertadvies zal extra aandacht zijn voor de volgende punten:

- de nieuwe versie van de standaard bevat breaking changes ten opzichte van de vorige versie en is daardoor niet backward compatible. In hoeverre is dit van invloed op draagvlak van OAS in de nieuwe versie, zowel voor organisaties als voor de relatie van OAS met andere standaarden op de 'pas toe of leg uit'-lijst?

- in hoeverre is Nederlandse deelname aan ontwikkeling en beheer van OAS wenselijk en welke mogelijkheden zijn er voor Nederlandse deelname aan ontwikkeling en beheer van OAS (incl. regierol voor Nederland voor stimuleren van adoptie)?
- in hoeverre zijn er raakvlakken met de Wet elektronische gegevensuitwisseling in de zorg, in het kader van wettelijke verplichting van OAS?

In de rest van dit document wordt het advies nader onderbouwd. Hoofdstuk 2 geeft een korte uitleg van de standaard en met name de versiewijziging. Hoofdstuk 3 beschrijft het proces waarmee dit advies tot stand kwam, alsmede de vervolgstappen. Hoofdstuk 4 toetst in hoeverre de nieuwe versie van de standaard voldoet aan de criteria om in behandeling genomen te worden door het Forum Standaardisatie. Hoofdstuk 5 verkent of er inhoudelijke belemmeringen bestaan die een positief expertadvies in de weg zouden kunnen staan.

Tenslotte wordt er in hoofdstuk 6 een praktijkvoorbeeld gegeven dat Forum Standaardisatie kan gebruiken om de maatschappelijke waarde van de nieuwe versie van de standaard te communiceren.

# 2 Korte beschrijving van de standaard

## 2.1 Over de standaard

Een OpenAPI Specification (OAS) beschrijft de eigenschappen van de data die een REST API als input accepteert en als output teruggeeft. Een API (Application Programming Interface) is een veel toegepaste en essentiële technologie om moderne applicaties (en databronnen) snel en effectief met elkaar te verbinden en om eenvoudig informatie uit te wisselen. Representational State Transfer (REST) is een ontwerpprincipe dat wereldwijd veel gebruikt wordt voor het bouwen van programmeerinterfaces over het web (API's). REST is geen standaard maar een ontwerpprincipe, en laat nog veel vrijheid in het structureren van API's.

OAS specificeert welke attributen de API verwerkt en hun datatypen, en niet welke implementatie er achter de API schuilgaat. OAS is dus een beschrijvende taal en heeft geen binding met specifieke programmeertalen. Daarnaast beschrijft OAS de security vereisten om toegang te krijgen tot de implementatie van de API. OAS 3.1 is de opvolger van OAS 3.0, welke reeds is opgenomen op de 'pas toe of leg uit'-lijst.

De technologie van API's is constant aan ontwikkeling onderhevig en het is belangrijk dat de een standaard hierop aansluit. De aanpassingen van OAS 3.1 ten opzichte van OAS 3.0 zijn in hoofdzaak de volgende:

- toevoeging van beschrijvingen van webhooks. Webhooks zijn geautomatiseerde berichten die gegevens overbrengen tussen applicaties wanneer er een wijziging plaatsvindt in de bronapplicatie.
- mogelijkheid om Mutual TLS te specificeren als 'Security Schema'. Mutual TLS is een veelgebruikte methode waarbij authenticatie in twee richtingen plaatsvindt.

Mutual TLS is ook een vereiste bij de implementatie van de nieuwe versie van Digikoppeling koppelvlak REST API. Dit was voor Logius een belangrijke reden om deze versiewijziging in te dienen voor plaatsing op de 'pas toe of leg uit'-lijst.

Versie 3.1 van OAS is niet backward compatible. De impact hiervan zal tijdens de expertbijeenkomst verder getoetst te worden. De specificatie van de standaard (migratie van JSON Schema Draft 5 naar JSON Schema Draft 12) is de basis van de breaking changes.

## 2.2 Waarom is deze standaard belangrijk?

OAS draagt bij aan betere gegevensuitwisseling tussen diverse partijen en betere toegankelijkheid van gegevens doordat OAS REST API's toegankelijker maakt door deze op een gestandaardiseerde manier te beschrijven. Een stabiele en eenduidige wijze van beschrijven van REST API's maakt het eenvoudiger om een API te documenteren. Dit bevordert het gebruik van API's.

REST API's worden in de praktijk op verschillende manieren gestructureerd en beschreven. Daardoor moeten softwareontwikkelaars de structuur van een REST API eerst verkennen en doorgronden voordat zij deze kunnen gebruiken. Het gebruik van REST API's is daardoor minder efficiënt dan wanneer er een standaard beschrijvingswijze voor REST API's wordt gebruikt.

De toepassing van de webhooks geeft een nieuwe dimensie aan de gegevensuitwisseling door partijen actief te informeren bij een wijziging van een gegeven in een bronregistratie. Dit leidt tot een accuratere dienstverlening en een mogelijke ontzorging van de burger (burger hoeft niet actief de wijzigingen door te geven). Mutual TLS verhoogt de beveiligingsgraad van de gegevensuitwisseling.

# 3 Betrokkenen en proces

Op 10 augustus 2022 heeft Logius de standaard OAS in de nieuwe versie 3.1 formeel aangemeld bij het Bureau Forum Standaardisatie middels het aanbieden van het ingevulde aanmeldformulier. Het betreft hier een versiewijziging van de OAS standaard, van versie 3.0 naar versie 3.1. Het Bureau Forum Standaardisatie heeft Lost Lemon de opdracht gegeven om de toetsing van de standaard te begeleiden.

Op dinsdag 20 september heeft het intakegesprek plaatsgevonden. Bij het online intake gesprek waren de volgende personen aanwezig:

- Martin van der Plas (Logius)
- Hans Laagland (Bureau Forum Standaardisatie, als toehoorder)
- Redouan Ahaloui (Bureau Forum Standaardisatie, als toehoorder)
- Jeroen de Ruig (Lost Lemon)
- Marieke Doorenbosch (Lost Lemon)

In dit gesprek is onderzocht of OAS in de nieuwe versie 3.1 voldoet aan de criteria om in procedure genomen te worden. Daarnaast is vooruitgeblikt op de procedure. Dit intake advies

is tot stand gekomen op basis van de informatie in het aanmeldformulier en de aanvullend verkregen informatie tijdens het intake gesprek en deskresearch.

# 4 Voldoet de standaard aan de criteria om in procedure genomen te worden?

Bij een versiewijziging is het doel om te onderzoeken of OAS in de nieuwe versie nog steeds voldoet aan de criteria ten opzichte van de huidige versie op de 'pas toe of leg uit'-lijst. Uit het intakegesprek kwam naar voren dat OAS in de nieuwe versie no steeds voldoet aan de vier criteria om in behandeling genomen te worden voor plaatsing op de 'pas toe of leg uit'-lijst. Hoe de standaard is getoetst op de vier criteria, wordt hieronder toegelicht in paragrafen 4.1-4.4.

## 4.1 Valt de standaard binnen de scope van Forum Standaardisatie?

Hier is niets aan veranderd ten opzichte van versie 3.0 van de standaard. OAS is van toepassing op de beschrijving van alle gegevensuitwisseling via REST API's van (semi)overheden met bedrijven, burgers of andere overheden. Daarmee valt de standaard binnen de scope van het Forum.

De standaard is uitgebreid met de mogelijkheid om webhooks te beschrijven. Daarnaast is in OAS 3.1 de mogelijkheid om Mutual TLS te specificeren als 'Security Schema' toegevoegd. De wijzigingen worden beoordeeld als een verrijking van de standaard en de standaard is daarbij nog beter ondersteunend bij het vormgeven van gegevensuitwisseling middels REST API.

## 4.2 Heeft de standaard een toepassing die een enkele organisatie of sector overstijgt?

Het functioneel toepassingsgebied en het organisatorisch werkingsgebied blijven onveranderd. De standaard is van toepassing voor alle overheden en instellingen uit de publieke sector die gegevensuitwisseling met andere overheden, instellingen, bedrijven en burgers via REST API's mogelijk willen maken. API's zijn niet gelimiteerd tot één specifiek domein, maar zorgen juist voor een koppeling van datastromen uit verschillende domeinen. Door de API's op een standaard wijze te beschrijven via OAS is het eenvoudiger om API's toe te passen en gegevens te delen.

Sinds het verplichten van de standaard OAS 3.0 via 'pas toe of leg uit'-verplichting is het aantal organisaties toegenomen dat REST API's heeft gepubliceerd. De verwachting is dat deze stijgende lijn door zal zetten met het blijven verplichten OAS 3.1 aan de overheid, omdat versie 3.1 een verdere verrijking is van de mogelijkheden ten opzicht van versie 3.0. Toetsing hiervan zal moeten plaatsvinden in de expertbijeenkomst.

## 4.3 Is de standaard al wettelijk verplicht?

Het is zinvol de standaard op te nemen, gezien het feit dat deze niet wettelijk verplicht is. De standaard zorgt via eenduidige beschrijving van REST API's dat de manier van communicatie via REST API's binnen en tussen overheden kan worden geharmoniseerd. De wijze waarop harmonisering plaatsvindt, wordt meestal niet in de wet vastgelegd. Er zijn raakvlakken met de Wet elektronische gegevensuitwisseling in de zorg. Dit punt zal worden getoetst tijdens de expertbijeenkomst.

De verwachting is dat het opnemen van de nieuwe versie van standaard op de 'pas toe of leg uit'-lijst de adoptie van deze standaard zal versnellen.

## 4.4 Draagt de standaard bij tot de oplossing van een bestaand probleem?

OAS 3.1 is een uitbreiding van de vorige versie OAS 3.0. Door het opnemen in de beschrijving van onder andere webhooks en Mutual TLS sluit deze standaard aan bij de huidige ontwikkelingen binnen het gebruik en ontwerpen van REST API's. OAS 3.1 is daarbij nog beter ondersteunend bij het vormgeven van gegevensuitwisseling middels REST API's.

API strategie voor de Nederlandse overheid omschrijft een API als een combinatie van technische bestanden, documentatie en andere ondersteuning die helpen bij het aanroepen van externe applicaties. OAS doet een poging om REST API's toegankelijker te maken door ze op een gestandaardiseerde manier te beschrijven.

# 5 Is er zicht op een positief expertadvies?

Als het Forum Standaardisatie de standaard in procedure neemt, gaat een groep experts de standaard toetsen op de vier inhoudelijke criteria voor opname op de lijst. Het Forum Standaardisatie neemt geen standaarden in procedure waarvan bij aanvang al vaststaat dat deze niet op een positief expertadvies kan rekenen. Daarom wordt in dit intakeadvies vooruitgeblikt op de vier inhoudelijke criteria.

Het intakeonderzoek heeft geen inhoudelijke criteria gevonden die een positief expertadvies voor plaatsing van OAS in de nieuwe versie 3.1 op de 'pas toe of leg uit'-lijst in de weg kan staan.

Dit wordt toegelicht in paragrafen 5.1-5.4.

## 5.1 Toegevoegde waarde

De internationale standaard OAS 3.1 heeft meerwaarde ten opzichte van OAS 3.0, omdat in deze nieuwe versie webhooks functionaliteit is toegevoegd. Met de opname van webhooks functionaliteit in versie 3.1 wordt het mogelijk om de beschrijving van API's te voorzien van een signaleringsfunctie. Dit betekent dat door toepassing van de webhooks actief een signaal wordt gegeven bij wijziging van een gegeven in de ontsloten registratie.

De mogelijkheid om Mutual TLS te specificeren voor een API, leidt tot meer eenduidigheid in de API security bij toepassing van Mutual TLS. OAS 3.1 op de 'pas toe of leg uit'-lijst harmoniseert met de standaard Digikoppeling waarin ook Mutual TLS vereist is.

Er zijn momenteel geen andere concurrerende standaarden die in aanmerking kunnen komen voor de opname op de lijst.

Er zijn geen risico's verbonden aan de standaard in de nieuwe versie. OAS 3.1 is alleen beschrijvend en beïnvloedt zo niet de runtime bevraging en security van een bestaande API's. De standaard kent zelf geen privacyrisico's, maar helpt wel om duidelijke privacygevoelige API interactie goed te beschrijven. De kosten zijn minimaal een bestaande OAS 3.0 publicatie bij een release geschikt te maken als OAS 3.1 publicatie.

De nieuwe versie van de standaard bevat breaking changes ten opzichte van de vorige versie en is daardoor niet backward compatible met de vorige versie.

## 5.2 Open standaardisatieproces

Open API Specification (OAS) wordt beheerd door het Open API Initiative (OAI). Het is een internationale standaard waar grote partijen gebruik van maken. Open API Initiative is een open community opgezet door de Linux Foundation waarbij het beheer en de ontwikkeling gebaseerd is op een open online dialoog met een community van gebruikers die via een kiessysteem kunnen meebepalen over de prioritering van issues. Het besluitvormingsproces is op deze manier toegankelijk voor alle belanghebbenden.

Tooling en documentatie voor het gebruik van de standaard is openbaar toegankelijk. Zie voor meer informatie: OAI/OpenApi-Specification. De specificaties van de standaard zijn gratis beschikbaar. Er is wel een licentie (Apache-2.0) van toepassing.

Het is mogelijk om actief deel te nemen aan doorontwikkeling en beheer van de standaard, waaronder via het leveren van bijdrages via GitHub. Het beleid voor versiebeheer is vastgelegd. De OpenAPI Initiative community kalender is een openbaar overzicht van bijeenkomsten van technische en andere belanghebbenden.

Aandachtspunt voor het expertonderzoek is in hoeverre de Nederlandse deelname aan ontwikkeling en beheer van OAS wenselijk en welke mogelijkheden zijn er voor Nederlandse deelname aan ontwikkeling en beheer van OAS (incl. regierol voor Nederland voor stimuleren van adoptie).

Er is financiering voor de ontwikkeling en het onderhoud van de standaard. Een open community initiatief heeft als consequentie dat het beheer niet duurzaam geïnstitutionaliseerd is en dat er daardoor geen garantie bestaat voor de continuïteit van het beheer in de toekomst. Dit brengt ook risico's met zich mee voor de vrije toegang tot documentatie op de lange termijn.

## 5.3 Draagvlak

Geonovum, de VNG en Logius (indiener) ondersteunen het indienen van de nieuwe versie van de standaard ondersteunen.

Op developer.overheid.nl staat een lijst van API's die (semi-)overheidsorganisaties in Nederland aanbieden. API's die gebruik maken van OAS zijn onder andere:

- Organisaties Overheid (VNG)
- Ondernemersplein API (Kamer van Koophandel Nederland)
- CBS OData (Centraal Bureau voor de Statistiek)
- BAG API Huidige Bevragingen (Basisregistratie Adressen en Gebouwen)(Dienst voor het kadaster en de openbare registers)
- CPA-register (Logius)

Deze API's zijn nu echter nog gebaseerd op OAS 3.0 en (nog) niet op de nieuwe versie OAS 3.1. Via developer.overheid.nl is op moment van opstellen van dit intakeadvies nog niet te meten of versie 3.0 of versie 3.1 wordt gebruikt. Versie 3.1 is gepubliceerd op 15 februari 2021, en dat is wellicht nog te kort om ook daadwerkelijk al diverse implementaties te hebben van de standaard.

Vanwege de toevoeging van webhooks en Mutual TLS aan OAS 3.0 is de verwachting dat de nieuwe versie snel in gebruik genomen gaat worden. Of deze verwachte toename ook klopt, zal moeten worden getoetst tijdens de expertbijeenkomst.

Beschrijvingen die zijn gemaakt met OAS 3.1 zijn niet backward compatible met de vorige versie. Dit kan van invloed zijn op het draagvlak. Expertonderzoek moet dit gaan uitwijzen. Een bestaande OAS 3.0 publicatie is bij een release eenvoudig geschikt te maken als OAS 3.1 publicatie. Zie hiervoor ook de migratie instructies op Openapis.org.

## 5.4 Opname op de lijst bevordert adoptie

De verwachting is dat de plaatsing van de versiewijziging van de standaard op de 'pas toe of leg uit'-lijst zal zorgen voor meer bekendheid van deze versie van de standaard. Daardoor zullen overheidsorganisaties de nieuwe versie (OAS 3.1) van de standaard gaan toepassen of toelichten waarom ze dit niet doen.

Een goede bekendmaking en duidelijk uitleg over de versiewijziging van de standaard zal hieraan bijdragen. Nederlandse deelname aan ontwikkeling en beheer van OAS (incl. regierol voor Nederland voor stimuleren van adoptie) kan hieraan bijdragen. Ook kan bijvoorbeeld het Kennisplatform API's een rol spelen in bevorderen van adoptie. Het Kennisplatform API's wil API's beter bij de vraag aan laten sluiten, kennis over het toepassen van API's uitwisselen en de aanpak bij verschillende organisaties op elkaar afstemmen en waar nodig standaardiseren.

# 6 Praktijkvoorbeeld

OpenAPI.tools biedt een overzicht van voorbeelden van OAS 3.1 compatible tools en API's.

Mutual TLS is een voorwaarde bij de implementatie van de nieuwe versie van Digikoppeling koppelvlak REST API. Dit was een belangrijke reden om deze versiewijziging van OAS in te dienen voor plaatsing op de 'pas toe of leg uit'-lijst. Dit praktijkvoorbeeld van OAS bij Digikoppeling wordt tijdens de expertbijeenkomst nader getoetst.

Met de opname van webhooks functionaliteit in versie 3.1 wordt het mogelijk om API's te voorzien van een signaleringsfunctie. Dit betekent dat door toepassing van de webhooks actief een signaal wordt gegeven bij wijziging van een gegeven in de ontsloten registratie. Een wijziging in een registratie kan directe gevolgen hebben voor het recht op een overheidsvoorziening. Denk bijvoorbeeld aan het wijzigen van een adres naar een andere gemeente of het overlijden van een persoon. Door gebruik te maken van webhooks worden afnemende organisaties van een gegeven actief geïnformeerd over een wijziging en kunnen ze vervolgens beoordelen of de persoon in kwestie nog recht heeft op een betreffende overheidsvoorziening. Dit zal worden getoetst bij de experts tijdens de expertbijeenkomst.