



Oplegnotitie open standaarden, lijsten

Vergadering: Forum Standaardisatie woensdag 24 september 2025

Agendapunt:

Documentnummer:

Aan: Forum Standaardisatie

Van: Stuurgroep Open Standaarden

Datum: 1 september 2025

Versie: 1.0

Bijlagen: Forumadvies NLGov profile for CloudEvents
Forumadvies NLGov REST API Design Rules 2.0
Intakeadvies STIX en TAXII 2.1
Intakeadvies DCAT-AP-NL 3.0
Intakeadvies NL-GOV-Assurance-profile-for-OAuth-2.0-versie-1.1

Rechten: [CC0 publieke domeinverklaring](#)

Ter besluitvorming

A. NLGov profile for CloudEvents verplichten aan de overheid, voor het notificeren over gebeurtenissen op wijzigingen in alle registers (Forumadvies)

[Bijlage: Forumadvies NLGov profile for CloudEvents]

Inleiding

Als overheidsorganisaties elkaar sneller en gestandaardiseerd notificeren over een plaatsgevonden gebeurtenis, kunnen zij daarop beter gebeurtenisgedreven actie ondernemen. Het toepassen van [NLGov profile for CloudEvents](#) helpt daarbij. Het verbetert de uitwisseling van gegevens en maakt de digitale overheid betrouwbaarder en wendbaarder.

Vraag aan Forum Standaardisatie om in te stemmen met de volgende adviezen aan het OBDO:

- NLGov profile for CloudEvents te verplichten aan de overheid ('Pas toe of leg uit') door deze te plaatsen op de 'Pas toe of leg uit'-lijst voor het sneller en gestandaardiseerd uitwisselen van gegevens over plaatsgevonden gebeurtenissen.
- Aan Logius het predicaat 'Uitstekend beheer' toe te kennen voor NLGov profile for CloudEvents

Het voorgestelde functioneel toepassingsgebied voor NLGov profile for CloudEvents is:

NL GOV profile for CloudEvents moet worden toegepast op het notificeren over gebeurtenissen op wijzigingen in alle registers.

Belang van de standaard: betere gegevensuitwisseling

Overheidsorganisaties hebben een groeiende behoefte aan actuele informatie vanuit databronnen. Gegevens veranderen vaak en snel, bijvoorbeeld bij verhuizingen of overlijden. Door NL GOV profile for CloudEvents toe te passen kunnen overheidsorganisaties elkaar gemakkelijker snel en gestandaardiseerd notificeren over dit soort gebeurtenissen die hebben plaatsgevonden. Dat helpt de overheid om sneller en beter te werken: signalen komen snel op de juiste plek terecht, waardoor organisaties sneller kunnen reageren, betere keuzes kunnen maken en aan de verwachtingen van burgers kunnen voldoen.

Afnemers zijn door de notificaties snel op de hoogte van relevante gebeurtenissen en kunnen daarop gebeurtenisgedreven actie ondernemen. Afhankelijk van de implementatie kan het ook bijdragen aan het realiseren van de uitgangspunten [Dataminimalisatie](#) en [Data bij de bron](#).

Meer over notificeren en de meerwaarde van deze standaard is beschreven op de website van de [NORA](#).

Hoe is het proces verlopen?

Logius heeft versie 1.0 van NL GOV profile for CloudEvents op 23 augustus 2024 aangemeld voor plaatsing op de 'Pas toe of leg uit'-lijst. Op basis van het [intakeadvies](#) heeft het Forum Standaardisatie op 4 december 2024 besloten de standaard in procedure te nemen.

De leden van de expertgroep zijn op 15 april 2025 bijeengekomen om de standaard te toetsen aan de criteria en geïdentificeerde aandachtspunten te bespreken. Tijdens deze bijeenkomst zijn ook het toepassings- en werkingsgebied vastgesteld. De uitkomst van het expertonderzoek is vastgelegd in het [expertadvies](#), dat het bureau ter openbare consultatie van 24 juni 2025 tot 5 augustus 2025 heeft gepubliceerd op [internetconsultatie.nl](#). Het Bureau Forum Standaardisatie publiceerde het expertadvies ter openbare consultatie via de website van [Internetconsultatie](#) van 24 juni tot 5 augustus 2025. Op basis van het expertadvies, de [reacties uit de consultatie](#) en inzichten van leden van het Forum Standaardisatie is het Forumadvies opgesteld.

Over de standaard

NLGov profile for CloudEvents is een set afspraken over hoe de Nederlandse overheid gebruik kan maken van de internationale standaard [CloudEvents](#). NL GOV profile for CloudEvents wordt een 'notificatiestandaard' genoemd. De standaard kan breder worden toegepast, maar het voorgestelde functioneel toepassingsgebied beperkt zich tot het gebruik van de standaard voor notificeren. De standaard beschrijft hoe informatie over een plaatsgevonden gebeurtenis gestandaardiseerd kan worden uitgewisseld met gebruik van verschillende gegevensformaten, transportprotocollen en voorzieningen.

NL GOV profile for CloudEvents is in beheer bij [Logius](#). De internationale standaard CloudEvents is ontwikkeld door de [Serverless Working Group](#) van de Cloud Native Computing Foundation.

B. NLGov REST API Design Rules 2.0 verplichten aan de overheid, voor uniform en eenduidig ontwerp van REST API's overheid (Forumadvies)

[Bijlage: Forumadvies NLGov REST API Design Rules 2.0]

Inleiding

Het is voor ontwikkelaars van REST API's voor de overheid makkelijker als deze allemaal volgens dezelfde basisregels en naamgeving worden gebouwd. Dit voorkomt een lappendeken van REST API's die moeilijk met elkaar kunnen communiceren. De standaard NLGov REST API Design Rules helpt ontwikkelaars op een uniforme en voorspelbare manier te ontwerpen. De aangemelde versie 2.0 van de standaard breidt de uniformiteit en eenduidigheid verder uit. De voorgaande versie (1.0) staat thans [geregistreerd](#) op de 'Pas toe of leg uit'-lijst.

Vraag aan Forum Standaardisatie om in te stemmen met de volgende adviezen aan het OBDO:

- Versie 2 van NLGov REST API Design Rules 2.0 te verplichten aan de overheid ('Pas toe of leg uit') door deze te plaatsen op de 'Pas toe of leg uit'-lijst voor het verder bevorderen van consistentie in het gegevenslandschap bij de digitale overheid.
- Aan Logius het predicaat 'Uitstekend beheer' toe te kennen voor NLGov REST API Design Rules

Belang van de standaard: betere gegevensuitwisseling

Het toepassen van NLGov REST API Design Rules helpt ontwikkelaars van REST API's (koppelvlakken over internet voor het bevragen van databronnen) op een uniforme en voorspelbare manier te ontwerpen. REST API's van de overheid krijgen tijdens het ontwerp en de ontwikkeling ervan door toepassing van deze standaard een meer eenduidige structuur, wat wildgroei aan structuren voorkomt. Versie 2.0 van de standaard NLGov REST API Design Rules draagt bij aan het verder bevorderen van consistentie in het gegevenslandschap bij de

digitale overheid. Dit zorgt voor een betere gegevensuitwisseling tussen overheidsorganisaties onderling en met bedrijven en burgers.

Hoe is het proces verlopen?

Logius heeft versie 2.0 van de standaard NLGov REST API Design Rules op 2 februari 2024 aangemeld voor plaatsing op de 'Pas toe of leg uit'-lijst. Op basis van het [intakeadvies](#) heeft het Forum Standaardisatie op 2 oktober 2024 besloten de standaard in procedure te nemen.

De leden van de expertgroep zijn op 22 mei 2025 bijeengekomen om de standaard te toetsen aan de criteria en geïdentificeerde aandachtspunten te bespreken. Tijdens deze bijeenkomst zijn ook het toepassings- en werkingsgebied vastgesteld. De uitkomst van het expertonderzoek is vastgelegd in het [expertadvies](#), dat het bureau ter openbare consultatie van 24 juni 2025 tot 5 augustus 2025 heeft gepubliceerd op internetconsultatie.nl. Op basis van het expertadvies, de [reacties uit de consultatie](#) en inzichten van leden van het Forum Standaardisatie is het Forumadvies opgesteld.

Over de standaard

NLGov REST API Design Rules 2.0 geeft een verzameling basisregels (design rules) voor structuur en naamgeving waarmee de overheid op een uniforme en eenduidige manier REST-API's aanbiedt. Dit maakt het voor ontwikkelaars gemakkelijker om betrouwbare applicaties te ontwikkelen met REST API's van de overheid.

In versie 2.0 zijn ten opzichte van versie 1.0 (die nu op de 'Pas toe of leg uit'-lijst staat) zowel technische als inhoudelijke verbeteringen verwerkt. Versie 2.0 is modulair opgebouwd om de standaard flexibeler en beter toepasbaar te maken in verschillende contexten. De semantic versioning is uitgebreid. En verplichte modules zoals "[Geospatial](#)" en "[Transport Security](#)" zijn toegevoegd. Daarnaast zijn ook expliciete instructies voor testbaarheid toegevoegd via [Developer.overheid.nl](https://developer.overheid.nl). De details van de wijzigingen in versie 2.0 zijn te vinden in de [release notes](#).

C. STIX en TAXII 2.1 verplichten aan de overheid, voor gestructureerde en automatische uitwisseling van cyberdreigingsinformatie tussen organisaties (intakeadvies)

[Bijlage: Intakeadvies STIX en TAXII 2.1]

Inleiding

Met de juiste informatie over mogelijke cyberdreigingen of -aanvallen kunnen overheidsorganisaties indien nodig tijdig en adequaat beveiligingsmaatregelen treffen. De standaarden [Structured Threat Information Expression](#) (STIX) en [Trusted Automated eXchange of Indicator Information](#) (TAXII) maken het mogelijk deze informatie op een

gestructureerde en automatisch verwerkbare manier te beschrijven en real-time te delen met belanghebbende organisaties. De voorgaande versies van STIX (versie 1.2.1) en TAXII (1.1.1) staan thans geregistreerd op de 'Pas toe of leg uit'-lijst onder de registratie [STIX en TAXII](#). STIX en TAXII versie 2.1 bieden ten opzichte van de vorige versies meerwaarde. De [standaarden zijn verbeterd op meerdere punten](#). Beide standaarden zijn in beheer bij de [Organization for the Advancement of Structured Information Standards](#) (OASIS).

Vraag aan Forum Standaardisatie om in te stemmen met het volgende advies:

Versies 2.1 van de standaarden **STIX en TAXII** in samenhang in procedure te nemen voor opname op de 'Pas toe of leg uit'-lijst. Een volledig expertonderzoek is aangewezen om de standaard te toetsen aan de criteria voor opname op de lijst (veiliger internet).

Belang van de standaard: veiliger internet

STIX heeft een belangrijke rol voor goede informatie-uitwisseling van cyberdreigingsinformatie, doordat het een consistent, gestructureerd en machineleesbaar formaat biedt om indicatoren, incidenten en dreigingsactoren eenduidig te beschrijven en delen. TAXII is ontworpen om de uitwisseling te ondersteunen van cyberdreigingsinformatie die in STIX wordt vertegenwoordigd. Door deze standaarden te implementeren zijn organisaties snel op de hoogte van cyberdreigingen. Dit verhoogt de cyberveiligheid en digitale weerbaarheid van de overheid en instellingen in de (semi-)publieke sector maar ook private sectoren.

Hoe is het proces verlopen?

Op 15 april 2025 heeft het Nationaal Cyber Security Centrum (NCSC) STIX en TAXII versie 2.1 aangemeld om te toetsen of de standaarden in de nieuwe versie geschikt zijn om te blijven verplichten ('Pas toe of leg uit') aan de overheid. Op 20 mei 2025 heeft een intakegesprek plaatsgevonden met de indiener, procedurebegeleider InnoValor Advies en Bureau Forum Standaardisatie. In dit gesprek is onderzocht of STIX en TAXII versie 2.1 voldoet aan de criteria om in procedure te worden genomen. De standaarden lijken te voldoen aan de criteria om in procedure te worden genomen. Dit intakeadvies is tot stand gekomen op basis van het intakeonderzoek.

D. DCAT-AP-NL 3.0 verplichten aan de overheid, voor gestandaardiseerde uitwisseling van metadata tussen verschillende dataportalen (intakeadvies)

[Bijlage: Intakeadvies DCAT-AP-NL 3.0]

Inleiding

Op dit moment gebruiken verschillende overheidsorganisaties uiteenlopende metadata-standaarden, wat het lastig maakt om gegevens over domeinen heen te vinden en te

hergebruiken. Dit belemmert zowel overheden als burgers in het zoeken naar betrouwbare en bruikbare data.

Door de implementatie van de standaard [DCAT-AP-NL 3.0](#) wordt metadata beter gestructureerd, consistent vastgelegd en eenduidig doorzoekbaar. Het gebruik van vaste waardenlijsten, bijvoorbeeld voor thema's en toegangsrestricties, draagt bovendien bij aan hogere kwaliteit en vergelijkbaarheid van metadata. DCAT-AP-NL 3.0 is in beheer bij Geonovum.

Vraag aan Forum Standaardisatie om in te stemmen met het volgende advies:

DCAT-AP-NL 3.0 in procedure te nemen voor opname op de 'Pas toe of leg uit'-lijst. Een volledig expertonderzoek is aangewezen om de standaard te toetsen aan de criteria voor opname op de lijst (betere gegevensuitwisseling).

Hoe is het proces verlopen?

Op 8 mei 2025 heeft Geonovum de standaard DCAT-AP-NL 3.0 aangemeld voor plaatsing op de 'Pas toe of leg uit' lijst. Op 3 juli 2025 heeft een intakegesprek plaatsgevonden met de indiener, procedurebegeleider InnoValor Advies en Bureau Forum Standaardisatie. In dit gesprek is verkend of de standaard DCAT-AP-NL 3.0 voldoet aan de criteria om in procedure te worden genomen. De standaard lijkt te voldoen aan de criteria om in procedure te worden genomen. Dit intakeadvies is tot stand gekomen op basis van het intakegesprek en aanvullend onderzoek.

Belang van de standaard: betere gegevensuitwisseling

Toepassing van DCAT-AP-NL 3.0 draagt bij aan openheid en transparantie van de Nederlandse overheid en digitale soevereiniteit (door controle over data-uitwisseling binnen nationale en Europese kaders). Momenteel wordt binnen de overheid gewerkt met uiteenlopende metadata-standaarden, wat zoekbaarheid en herbruikbaarheid belemmert. Door toepassing van DCAT-AP-NL 3.0 en het gebruik van vaste waardenlijsten, bijvoorbeeld voor thema's en toegangsrestricties, ontstaat er meer uniformiteit in metadatering.

E. NL GOV Assurance profile for OAuth 2.0 versie 1.1 verplichten aan de overheid, voor het veilig autoriseren van toegang tot gegevens via een REST API (intakeadvies)

[Bijlage: NL GOV Assurance profile for OAuth 2.0 versie 1.1]

Inleiding

NL GOV Assurance profile for OAuth 2.0 legt bindende afspraken vast over het gebruik van de standaard OAuth 2.0 bij de Nederlandse overheid. OAuth 2.0 is een open standaard voor de

beveiliging van applicaties die gegevens uitwisselen met behulp van REST APIs. Met OAuth 2.0 kunnen gebruikers een website of webapplicatie autoriseren om hun persoonlijke gegevens via een REST API op te halen bij een ander systeem, zonder daarbij hun gebruikersnaam en wachtwoord uit handen te geven. In combinatie met onderliggende standaard OAuth 2.0 zorgt NL GOV Assurance profile for OAuth 2.0 ervoor dat de autorisatie van gebruikers van REST APIs van de overheid op een uniforme en eenduidige plaatsvindt.

De nieuw aangemelde versie (1.1) is een kleine, incrementele update ten opzichte van de vorige versie en maakt duidelijk welke content specifiek Nederlands is en welke content nog overeenkomt met de internationale basis (OAuth2.0). De voorgaande versie (1.0) staat thans [geregistreerd](#) op de 'Pas toe of leg uit'-lijst.

Vraag aan Forum Standaardisatie om in te stemmen met het volgende advies:

NL GOV Assurance profile for OAuth 2.0 versie 1.1 in procedure te nemen voor opname op de 'Pas toe of leg uit'-lijst. Een verkort expertonderzoek is aangewezen om de standaard te toetsen aan de criteria voor opname op de lijst (betere gegevensuitwisseling).

Hoe is het proces verlopen?

Op 20 december 2024 heeft Logius het NL Gov Assurance profile for OAuth 2.0 versie 1.1 aangemeld voor plaatsing op de 'Pas toe of leg uit' lijst. Omdat het om een beperkte versiewijziging gaat, is afgestemd de besluitvorming van het Forum Standaardisatie en het OBDO af te wachten over het voorstel (thans geaccordeerd) om de procedures voor beperkte versiewijzigingen te verkorten. Op 14 augustus 2025 heeft een intakegesprek plaatsgevonden met de indiener, procedurebegeleider InnoValor Advies en Bureau Forum Standaardisatie. In dit gesprek is onderzocht of NL Gov Assurance profile for OAuth 2.0 versie 1.1 voldoet aan de criteria om in procedure te worden genomen. De standaard lijkt te voldoen aan de criteria om in procedure te worden genomen. Dit intakeadvies is tot stand gekomen op basis van het intakeonderzoek.

Belang van de standaard: betere gegevensuitwisseling

Het nut van de nieuwe versie (1.1) ligt in het verbeteren van interoperabiliteit van en veiligheid van authenticatie en toegang tot gegevensbronnen. Door duidelijk onderscheid te maken tussen wat specifiek Nederlands is en wat internationaal toepasbaar is, sluiten Nederlandse oplossingen beter aan bij de rest van Europa en daarbuiten. Daarnaast is een nieuw profiel toegevoegd (client credentials profiel) dat ook systemen zonder gebruikers inlog (user OAuth) toegang kan geven tot gegevensbronnen. Dit vergroot de mogelijkheid om processen efficiënter te automatiseren en diensten betrouwbaarder en veiliger aan te bieden.