



Expertadvies NL Gov Assurance Profile for OAuth 2.0 versie 1.1.0

Aan:	Forum Standaardisatie
Van:	Innovalor Advies B.V.
Datum:	6 maart 2026
Versie:	1.0
Bijlagen:	

1 Advies

De experts die betrokken waren bij het expertonderzoek adviseren om NL Gov Assurance Profile for OAuth 2.0 versie 1.1.0 te verplichten ('Pas toe of leg uit') via plaatsing op de 'Pas toe of leg uit'-lijst van het Forum Standaardisatie. De wijzigingen in de nieuwe versie hebben voor het huidige functioneel toepassingsgebied geen gevolgen. Het voorgestelde functioneel toepassingsgebied voor NL Gov Assurance Profile for OAuth 2.0 versie 1.1.0 blijft daarmee:

NL Gov Assurance Profile for OAuth 2.0 versie 1.1.0 moet worden toegepast op applicaties waarbij gebruikers of 'resource owners' impliciet of expliciet toestemming geven aan een dienst van een derde om namens deze toegang te krijgen tot gegevens via een REST API's waarvoor ze recht van toegang hebben

De experts adviseerden Logius tijdens de expertbijeenkomst van 11 december 2025 het functioneel toepassingsgebied te wijzigen omdat dit als onvoldoende werd beoordeeld. Om het huidige functioneel toepassingsgebied nader toe te lichten heeft er een extra bijeenkomst betreft het functioneel toepassingsgebied plaatsgevonden. Toelichting hierop is opgenomen in hoofdstuk 5.1.2.1.

De experts komen tot de conclusie dat NL Gov Assurance Profile for OAuth 2.0 versie 1.1.0 voldoet aan het criterium 'Open standaardisatieproces. Ook spreken de experts het vertrouwen uit in het open standaardisatieproces van de beheerder van de standaard om het predicaat Uitstekend beheer toe te kunnen kennen aan de beheerder voor deze standaard.

Tijdens de intakefase van de standaard zijn een aantal punten benoemd die in dit expertonderzoek nader zijn bekeken:

- Duidelijkheid en duurzaamheid van de naamgeving

- Duiding van welk relevant/bestaand probleem de nieuwe versie oplost
- De indiener (Logius) heeft tijdens de intake de wens voor het Predicaat 'Uitstekend beheer' uitgesproken
- Adoptie en betrokkenheid van organisaties uit het organisatorisch toepassingsgebied
- Impact van het verplichten van de NL-profiel op de onderliggende standaard die nu op de Aanbevolen-lijst staat
- Aankomende versies (1.2/2.1) die Logius beoogt aan te melden voor de 'Pas toe of leg uit'-lijst

In de rest van dit document wordt dit advies nader onderbouwd. Hoofdstuk 2 geeft een korte beschrijving van het nut en belang van de standaard. Hoofdstuk 3 beschrijft het proces waarmee dit advies tot stand kwam, alsmede de vervolgstappen. Hoofdstuk 4 geeft de samenstelling van de expertgroep weer. Hoofdstuk 5 documenteert hoe de experts de standaard beoordelen tegen de criteria voor opname op de lijst.

Tot slot geeft hoofdstuk 6 aanvullende adviezen van de experts aan het Forum Standaardisatie en het Overheidsbreed Beleidsoverleg Digitale Overheid (OBDO) om de adoptie van de standaard te stimuleren.

2 Korte beschrijving van de standaard

2.1 Over de standaard

De standaard [NL Gov Assurance profile for OAuth 2.0](#) legt bindende afspraken vast over hoe de Internationale standaard: [International Government Assurance Profile for OAuth 2.0](#) (IGov OAuth 2.0), moet worden toegepast binnen de Nederlandse overheid. Zo bepaalt de standaard hoe applicaties zich bij elkaar moeten registreren en hoe autorisatiecodes veilig uitgewisseld moeten worden. NL Gov Assurance profile for OAuth 2.0 is een Nederlands profiel op de internationale standaard IGov OAuth 2.0.

Met NL Gov Assurance profile for 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.

De aangemelde versie (1.1.0) van NL Gov Assurance profile for OAuth 2.0 is een incrementele update ten opzichte van versie 1.0 die nu de status 'Pas toe of leg uit' kent. De belangrijkste toevoeging is dat nu ook systemen die geen gebruik maken van user OAuth (bijvoorbeeld geautomatiseerde systemen zonder tussenkomst van een eindgebruiker) op een gestandaardiseerde manier toegang kunnen krijgen tot gegevensbronnen. Dit vergroot de interoperabiliteit en herbruikbaarheid van overheidsdata, en maakt het eenvoudiger voor systemen om met elkaar samen te werken.

2.2 Waarom is deze standaard belangrijk?

Het nut van versie 1.1.0 ligt in het verbeteren van interoperabiliteit van en veiligheid van authenticatie en toegang tot gegevensbronnen. De belangrijkste toevoeging is dat systemen die geen gebruik maken van user OAuth (bijvoorbeeld geautomatiseerde systemen zonder tussenkomst van een eindgebruiker) op een gestandaardiseerde manier toegang kunnen

krijgen tot gegevensbronnen. Dit vergroot de mogelijkheid om processen efficiënter te automatiseren en diensten betrouwbaarder en veiliger aan te bieden. Verder maakt de Versie 1.1.0 van de standaard het mogelijk om binnen bestaande internationale OAuth profielen gegevens veilig uit te wisselen zowel client-2-machine als machine-2-machine.

3 Betrokkenen en proces

Op 20 december 2024 heeft Logius NL Gov Assurance profile for OAuth 2.0 versie 1.1.0 aangemeld voor plaatsing op de 'Pas toe of leg uit'-lijst.

Op 14 augustus 2025 heeft een intakegesprek plaatsgevonden met de indiener, de procedurebegeleider en Bureau Forum Standaardisatie. In dit gesprek is verkend of NL Gov Assurance profile for OAuth 2.0 versie 1.1.0 voldoet aan de criteria om in procedure te worden genomen. De resultaten van het onderzoek zijn vastgelegd in het [intakeadvies](#). Op basis van dit intakeadvies heeft het Forum Standaardisatie op woensdag 25 september 2025 besloten de aanmelding in procedure te nemen.

Vervolgens heeft de procedurebegeleider in overleg met de indiener en Bureau Forum Standaardisatie een expertgroep samengesteld en een voorzitter aangesteld om de standaard in een expertsessie nader te bespreken.

Voorafgaand aan de expertbijeenkomst hebben de leden van de expertgroep een concept-expertadvies gekregen dat is samengesteld met informatie uit de aanmelding en het intake-onderzoek.

De leden van de expertgroep zijn op 11 december 2025 bijeengekomen om de bevindingen in het algemeen en de geïdentificeerde aandachtspunten in het bijzonder te bespreken. Tijdens deze bijeenkomst zijn ook het functioneel toepassingsgebied en het organisatorisch werkingsgebied vastgesteld. Op 26 februari 2027 zijn (een aantal) leden van de expertgroep bijeengekomen om het functioneel toepassingsgebied nader te bespreken. Tijdens deze bijeenkomst heeft Logius het huidige functioneel toepassingsgebied toegelicht en hebben de experts zich hierover uitgesproken met een definitief advies.

Dit expertadvies geeft de uitkomst van de expertsessie weer.

Het Bureau Forum Standaardisatie publiceert dit expertadvies ter openbare consultatie via de [website van Internetconsultatie](#). Gedurende de consultatieperiode kan iedereen op het expertadvies reageren.

Na afsluiting van de openbare consultatie ontvangen de leden van de expertgroep en de indiener een terugkoppeling over de reactie(s). Indien nodig kan dit aanleiding geven tot een aanvullend expertonderzoek.

Het Forum Standaardisatie formuleert op basis van het expertadvies, de reactie(s) uit de openbare consultatie en inzichten van de leden van het Forum Standaardisatie zelf een advies aan het Overheidsbreed Beleidsoverleg Digitale Overheid (OBDO). Het OBDO besluit om het advies wel of niet over te nemen.

4 Samenstelling van de expertgroep

Forum Standaardisatie streeft naar een samenstelling van de expertgroep met een evenwichtige publiek-private vertegenwoordiging van (toekomstige) gebruikers, leveranciers, wetenschappers en andere belanghebbenden. De expertgroep heeft een onafhankelijk voorzitter die de expertbijeenkomst leidt.

Aan de expertsessie hebben de volgende personen deelgenomen:

- Mironov, Stas (Logius, indiener)
- Beer de, Jeroen (Anoigo)
- Borgman, Martin (Kadaster)
- Kodden, Harry (SURF)
- Kok de, André (RVIG)
- Reinhoud, Erwin (Kennisnet)
- Terpstra, Frank (Geonovum)

Claudia Vermeulen, Managing Partner en Cigdem de Jongh adviseur bij InnoValor Advies, hebben de procedure in opdracht van het Bureau Forum Standaardisatie begeleid. Joram Verspaget en Wouter Kobes van het Bureau Forum Standaardisatie waren als toehoorder bij de expertbijeenkomst aanwezig.

5 Toetsing op inhoudelijke criteria

Het Forum Standaardisatie hanteert vier inhoudelijke hoofdcriteria om te bepalen of een standaard in aanmerking komt voor verplichten aan de overheid ('Pas toe of leg uit'-verplichting) via plaatsing op de 'Pas toe of leg uit'-lijst van Forum Standaardisatie:

1. Heeft de standaard toegevoegde waarde?
2. Zijn de standaard en het standaardisatieproces voldoende open?
3. Heeft de standaard voldoende draagvlak?
4. Bevordert opname van de standaard op de 'Pas toe of leg uit'-lijst of de lijst aanbevolen standaarden de adoptie?

Ieder van deze hoofdcriteria heeft deelcriteria [die beschreven staan op de website van het Forum Standaardisatie](#). Dit hoofdstuk beschrijft per criterium het resultaat van de toetsing.

5.1 Toegevoegde waarde

Met dit criterium wordt bepaald of het toepassingsgebied van de standaard duidelijk is, of deze zich goed verhoudt tot andere standaarden die al dan niet op de lijst staan, of de standaard een duidelijke meerwaarde heeft en of deze opweegt tegen eventuele risico's en nadelen.

5.1.1 Waardering van het criterium criteria 'Toegevoegde waarde'

De experts komen tot de conclusie dat NL Gov Assurance Profile for OAuth 2.0 versie 1.1.0 voldoet aan het criterium 'toegevoegde waarde'. Deze conclusie wordt in de volgende paragrafen toegelicht."

5.1.2 Is het toepassings- en werkingsgebied van de aanmelding goed gedefinieerd?

5.1.2.1 Is het functioneel toepassingsgebied goed gedefinieerd?

Het opgestelde functioneel toepassingsgebied voor NL Gov Assurance Profile for OAuth 2.0 versie 1.1.0 op de 'Pas toe of leg uit'-lijst is:

NL Gov Assurance Profile for OAuth 2.0 versie 1.1.0 moet worden toegepast op applicaties waarbij gebruikers of 'resource owners' impliciet of expliciet toestemming geven aan een dienst van een derde om namens deze toegang te krijgen tot gegevens via een REST API's waarvoor ze recht van toegang hebben

Het functioneel toepassingsgebied van de standaard is onveranderd ten opzichte van de voorgaande versie, de experts hebben tijdens de expertbijeenkomst van 11 december 2025 beoordeeld dat het functioneel toepassingsgebied onvoldoende duidelijk is en daarom herschreven moet worden. De experts adviseren de indiener het functioneel toepassingsgebied te wijzigen.

De indiener (Logius) wens desondanks het advies van 11 december 2025 het huidige functioneel toepassingsgebied niet te wijzigen. Om, specifiek, het functioneel toepassingsgebied nader te bespreken is de expertgroep op 28 februari 2026 bijeengekomen. Tijdens de extra bijeenkomst heeft Logius het functioneel toepassingsgebied en de relatie van NL Gov Assurance Profile for OAuth 2.0 versie 1.1.0 tot andere standaarden verder toegelicht. De experts concluderen aan de hand van de toelichting van Logius dat het huidige functioneel toepassingsgebied voldoende duidelijk is en het verplichte gebruik van de standaard eenduidig beschrijft.

5.1.2.2 Is het organisatorisch werkingsgebied goed gedefinieerd?

Het voorgestelde organisatorisch werkingsgebied voor NL Gov Assurance Profile for OAuth 2.0 versie 1.1.0 op de 'Pas toe of leg uit'-lijst is:

Nederlandse overheden (Rijk, provincies, gemeenten en waterschappen) en instellingen uit de (semi-)publieke sector.

Dit is het gangbare organisatorisch werkingsgebied voor standaarden op de 'Pas toe of leg uit'-lijst van het Forum Standaardisatie.

Het geformuleerde organisatorisch werkingsgebied van de standaard is voldoende breed om substantieel bij te dragen aan de interoperabiliteit van de (semi-)overheid. De functionele toepassing van de standaard overstijgt het organisatorisch werkingsgebied van een enkele organisatie of sector.

5.1.2.3 Is de standaard generiek toepasbaar (en niet alleen bedoeld voor gegevensuitwisseling met één of een beperkt aantal specifieke organisaties)?

Ja, de standaard kan over de grenzen van organisaties of sectoren worden gebruikt en is niet alleen bedoeld voor gegevensuitwisseling binnen één organisatie of sector. De toepassing van

de standaard overstijgt een enkele organisatie of sector. De standaard NL Gov Assurance Profile for OAuth 2.0 versie 1.1.0 moet worden toegepast bij applicaties waarbij gebruikers of 'resource owners' – expliciet of impliciet toestemming geven aan een dienst van een derde partij om namens deze toegang te krijgen tot gegevens via REST API's waarvoor zij recht van toegang hebben. Dit geldt zowel voor client-2-machine- als machine-2-machine-communicatie.

5.1.3 Verhoudt de standaard zich goed tot andere standaarden?

5.1.3.1 Kan de standaard naast of in combinatie met reeds opgenomen standaarden worden toegepast?

Ja, de standaard overlapt niet met bestaande standaarden op de lijst en conflicteert ook niet. De standaard sluit aan op de voorgaande versie (1.0) en op de internationale standaard [IGov OAuth 2.0](#).

5.1.3.2 Biedt de aangemelde standaard meerwaarde boven reeds opgenomen standaarden met een overlappend functioneel toepassings- en organisatorisch werkingsgebied?

Niet van toepassing, er zijn geen standaarden op de lijst met een overlappend functioneel toepassingsgebied.

5.1.3.3 Biedt de aangemelde standaard meerwaarde boven bestaande concurrerende standaarden die in aanmerking zouden kunnen komen voor opname?

Niet van toepassing, er zijn geen concurrerende open standaarden bekend die dezelfde functionele en organisatorische scope hebben.

5.1.3.4 Is de standaard een internationale standaard of sluit de standaard aan bij relevante internationale standaarden?

Ja, de standaard is een profiel op de Internationale standaard [IGov OAuth 2.0](#), ook zijn er Europese standaarden waar [IGov OAuth 2.0](#) op aansluit.

5.1.4 Wegen de voordelen van de standaard op tegen de nadelen?

5.1.4.1 Zijn de kosten van implementatie acceptabel en zijn deze kosten bekend en inzichtelijk?

Ja, er zijn geen kosten aan de implementatie van de standaard verbonden. De experts schatten dat de interne implementatie kosten acceptabel zijn, maar deze zijn niet specifiek bekend.

5.1.4.2 Is er een (kwalitatieve) businesscase van de standaard aanwezig?

Onbekend bij de experts.

5.1.4.3 Is de meerwaarde van de standaard goed inzichtelijk te maken?

Ja, de standaard levert een duidelijke en uitlegbare interoperabiliteitswinst op. Door de herziene opmaak van de standaard is er een duidelijk onderscheid te maken tussen welke content specifiek Nederlands is en welke content nog overeenkomt met de internationale

basis. Daarnaast is een nieuw profiel toegevoegd (client credentials profiel) dat ook systemen zonder gebruikers inlog (user OAuth) toegang kan geven tot gegeven bronnen. Dit vergroot de mogelijkheid om processen efficiënter te automatiseren en diensten betrouwbaarder en veiliger aan te bieden.

5.1.4.4 Zijn de beveiligingsrisico's aan overheidsbrede adoptie van de standaard acceptabel?

Ja, volgens de experts brengt de standaard geen veiligheidsrisico's met zich mee. En de baten van adoptie wegen zowel maatschappelijk als voor de overheid op tegen de mogelijke risico's.

5.1.4.5 Zijn de privacyrisico's aan overheidsbrede adoptie van de standaard acceptabel?

Ja, de experts hebben geen kennis van privacyrisico's die het gebruik van deze standaard met zich mee zou kunnen brengen.

5.2 Open standaardisatieproces

Met dit criterium wordt bepaald of het beheer en de (door)ontwikkeling van de standaard op een open, toegankelijke, inzichtelijke, zorgvuldige en duurzame wijze zijn ingericht.

5.2.1 Waardering van het criterium criteria 'Open standaardisatieproces'

De experts komen tot de conclusie dat NL Gov Assurance Profile for OAuth 2.0 versie 1.1.0 voldoet aan het criterium 'Open standaardisatieproces'. Deze conclusie wordt in de volgende paragrafen toegelicht. Ook spreken de experts het vertrouwen uit in het open standaardisatieproces van de beheerder van de standaard om het predicaat Uitstekend beheer toe te kunnen kennen aan de beheerder voor deze standaard.

5.2.2 Is de documentatie voor eenieder drempelvrij beschikbaar?

5.2.2.1 Is het specificatiedocument zonder belemmeringen beschikbaar?

Ja, het [specificatiedocument](#) is kosteloos beschikbaar. Ook het [specificatiedocument](#) van de onderliggende standaard, IGov OAuth 2.0 is kosteloos beschikbaar.

5.2.2.2 Is de documentatie over het ontwikkel- en beheerproces beschikbaar zonder dat er sprake is van belemmeringen?

Ja, de documentatie van de standaard is kosteloos en vrij beschikbaar. Het [beheerproces](#) is vrij beschikbaar evenals aanvullende documentatie over het ontwikkelproces. In de [GitHub repository](#) zijn ook overleggen en besluitvorming inzichtelijk.

5.2.3 Is het intellectuele eigendomsrecht voor eenieder beschikbaar, zodat de standaard vrij implementeerbaar en te gebruiken is?

5.2.3.1 Stelt de standaardisatieorganisatie het intellectueel eigendomsrecht op de standaard onherroepelijk royalty-free voor eenieder beschikbaar?

Ja, het intellectueel eigendomsrecht is onherroepelijk vrijgegeven en er zijn geen patenten of licenties bekend die met NL Gov Assurance Profile for OAuth 2.0 versie 1.1.0 zijn verbonden.

5.2.3.2 *Garandeert de standaardisatieorganisatie dat partijen die bijdragen aan de ontwikkeling van de standaard hun intellectueel eigendomsrecht voor (onderdelen van) de standaard onherroepelijk royalty-free voor eenieder beschikbaar stellen?*

Ja, de standaard valt onder een [Creative Commons Attribution 4.0 License](#). Dit betekent dat het werk onder de volgende voorwaarden mag worden gedeeld en gebruikt: bronvermelding, link naar licentie, wijzigingen vermelden.

5.2.4 *Is de inspraak van eenieder in voldoende mate geborgd?*

5.2.4.1 *Is het besluitvormingsproces toegankelijk voor alle belanghebbenden?*

Ja, het besluitvormingsproces is gebaseerd op consensus. Beheerder Logius maakt hiervoor gebruik van de governance van Generieke Digitale Infrastructuur (GDI) en neemt hierin de rol van onafhankelijke, duurzame beheerpartij en facilitator. Volgende versies zullen ook via de governance van de GDI worden vastgesteld. Deze governance-structuur kent brede vertegenwoordiging vanuit stakeholders in de e-overheid. Nadere details van de governance van het besluitvormingsproces zijn te lezen in paragraaf 2.2 van het REST API standaarden [beheerdocument](#) van Logius en is vrij toegankelijk voor alle belanghebbenden.

5.2.4.2 *Vindt besluitvorming plaats op een wijze die zoveel mogelijk recht doet aan de verschillende belangen?*

Ja, besluitvorming vindt plaats op basis van consensus. Mocht consensus niet mogelijk zijn, dan gaat het vraagstuk met een weergave van de verschillende standpunten door naar het eerstvolgend hoger gelegen gremium zoals beschreven in paragraaf 2.2.2 van het [beheerdocument](#).

5.2.4.3 *Kan een belanghebbende formeel bezwaar aantekenen tegen de gevolgde procedure?*

Ja, dit is mogelijk. Het inbrengen van formeel bezwaar is als begrip niet onderkend. Er is wel inbreng mogelijk rechtstreeks bij de beheerorganisatie. Klachten over de opzet of uitvoering van het beheerproces kunnen ingediend worden bij Logius.

5.2.4.4 *Organiseert de standaardisatieorganisatie regelmatig overleggen met belanghebbenden over doorontwikkeling en beheer van de standaard?*

Ja, Logius organiseert één keer per kwartaal overleggen met belanghebbenden over de doorontwikkeling en het beheer van de standaard. De [documentatie](#) van de overleggen is online vrij beschikbaar.

5.2.4.5 *Organiseert de standaardisatieorganisatie een openbare consultatie voordat (een nieuwe versie van) de standaard wordt vastgesteld?*

Ja, dit is onderdeel van het beheerproces van Logius. Uitbreidingen en aanpassingen in de REST API-standaarden komen tot stand door participatie van de verschillende belanghebbenden. De community bestaat uit eenieder die belanghebbende of belangstellende is met betrekking tot de standaard. Deelname aan de community kent geen drempels of restricties. Leden van de community kunnen alle informatie m.b.t. de standaard en het

beheer daarvan inzien via de website en via verschillende kanalen issues melden. Daarnaast kunnen community leden reageren op openbare consultaties.

5.2.5 Is de standaardisatieorganisatie onafhankelijk en duurzaam?

5.2.5.1 Is de ontwikkeling en het beheer van de standaard belegd bij een onafhankelijke non-profit standaardisatieorganisatie?

Ja, het beheer van de open standaard heeft een open governance en een open procedure voor belanghebbenden om te kunnen participeren in het beheer. Logius neemt hierin de rol van onafhankelijke, duurzame beheerpartij en facilitator. Logius volgt de governance van de [Generieke Digitale Infrastructuur \(GDI\)](#).

5.2.5.2 Is de financiering van de ontwikkeling en het onderhoud van de standaard voor ten minste drie jaar gegarandeerd?

Ja, de versievernieuwing valt onder het beheer van de standaard en het beheer van de REST API Standaarden (waaronder NLGov REST API Design Rules) is onderdeel van de structurele financiering en is structureel geregeld vanuit het Beheer & Exploitatie budget van Logius.

5.2.6 Is het (versie)beheer van de standaard goed geregeld?

5.2.6.1 Heeft de standaardisatieorganisatie gepubliceerd beleid met betrekking tot (versie)beheer van de standaard?

Ja, het beleid van de NL Gov Assurance Profile for OAuth 2.0 versie 1.1.0 valt onder het beheer van Logius. Dit beleid staat beschreven in het [beheerplan](#).

5.2.6.2 Is de beheerdocumentatie goed vindbaar en verkrijgbaar?

Ja, de [documentatie](#) van het beheer is online vrij beschikbaar.

5.2.6.3 Is het belang van de Nederlandse overheid voldoende geborgd bij de ontwikkeling en het beheer van de standaard?

Ja, het belang van de Nederlandse overheid is voldoende geborgd bij het ontwikkelen en het beheren van de standaard. Dit gebeurt o.a. via het Technisch Overleg (TO) van Logius waar verschillende stakeholders de belangen van de Nederlandse overheid borgen. Ook binnen de werkgroep beveiliging van het [Kennisplatform API's](#) wordt het belang van de Nederlandse overheid voldoende geborgd.

5.2.6.4 Is de vertegenwoordiging van belanghebbenden bij het beheer van de standaard een goede representatie van het werkingsgebied en functioneel toepassingsgebied van de standaard?

Ja, belanghebbende worden altijd uitgenodigd voor deze overleggen, maar de aanwezigen verschillen vaak afhankelijk van de wijzigingen die besproken worden. Het beheer is zodanig open ingericht en open gecommuniceerd door middel van een uitgebreide verzendlijst, dat alle belanghebbenden de kans hebben deel te nemen aan het beheer. Welke belanghebbende uitgenodigd zijn en welke aanwezig zijn wordt bijgehouden.

5.2.6.5 *Is het standaardisatieproces van de standaardisatieorganisatie zodanig goed geregeld dat het Forum zich kan onthouden van aanvullende toetsing bij de aanmelding van een nieuwe versie van de standaard?*

Ja, in het [beheerplan](#) staat beschreven dat bij het beheer van de REST API Standaarden verschillende gremia wordt onderscheiden die gezamenlijk invulling geven aan de governance op de standaard. Een onderdeel hiervan is het TO en het Meerjarenprogramma Infrastructuur Digitale Overheid (MIDO) Structuur. Dit overleg is verantwoordelijk voor het vaststellen van de doorontwikkel-roadmap en het vaststellen van major en minor releases van de standaard

5.2.7 *Is er adoptieondersteuning voor de standaard?*

5.2.7.1 *Is er een toegankelijk aanspreekpunt of organisatie waar meer informatie over de standaard is te vinden en op te vragen is?*

Ja, Logius is het aanspreekpunt voor meer informatie.

5.2.7.2 *Wordt er ondersteuning gegeven in de adoptie en de implementatie van de standaard?*

Ja, vragen en issues worden door de beheerder (Logius) opgepakt en beantwoord. Maar implementatie ondersteuning wordt inhouse of door marktondersteuners aangeboden.

5.3 Draagvlak

Met dit criterium wordt bepaald of de opname van de standaard op de 'Pas toe of leg uit'-lijst of lijst aanbevolen standaarden op voldoende breed draagvlak kan rekenen binnen de overheid. Een voorwaarde hierbij is ook dat er voldoende marktondersteuning voor de standaard bestaat en dat het marktaanbod evenwichtig is (dus geen leveranciersafhankelijkheid in de hand werkt).

5.3.1 *Waardering van het criterium criteria 'Draagvlak'*

De experts komen tot de conclusie dat NL Gov Assurance Profile for OAuth 2.0 versie 1.1.0 voldoet aan het criterium 'Draagvlak'. Deze conclusie wordt in de volgende paragrafen toegelicht.

5.3.2 *Bestaat er voldoende marktondersteuning voor de standaard?*

5.3.2.1 *Bieden meerdere leveranciers ondersteuning voor de standaard?*

Ja, er is voor de implementatie van Profiel OAuth-NL versie 1.1.0 voldoende marktondersteuning. De standaard is een profiel op het International profiel OAuth 2.0 wat veel wordt gebruikt en heeft daarom zowel Nederlandse als Internationale leveranciers.

5.3.2.2 *Kan een gebruiker de conformiteit van de implementatie van de standaard (laten) toetsen?*

Nee, er zijn geen toolings bekend bij de experts voor het NL Gov profiel. Wel zijn er voldoende [conformiteitstesten](#) beschikbaar voor de internationale standaard.

5.3.2.3 Draagt de standaard voldoende bij aan interoperabiliteit zonder dat aanvullende standaardisatieafspraken (zoals lokale profielen) noodzakelijk zijn om de standaard te implementeren of te gebruiken?

Ja, deze standaard is een lokaal profiel gericht op de Nederlandse overheid, wat per definitie bijdraagt aan de interoperabiliteit.

5.3.2.4 Zijn er profielen of voorbeeldimplementaties van de standaard aanwezig en zijn deze vrij te gebruiken?

Er zijn geen profielen of voorbeeld implementaties voor het profiel NL Gov Assurance profile for OAuth 2.0 versie 1.1.0 bekend. Wel zijn er voldoende use cases beschikbaar voor de onderliggende IGov OAuth 2.0 standaard met beschrijvingen van de 'client credential flow' en 'authorization code flow' via [Developer.overheid](#). De beheerder (Logius) biedt zelf geen voorbeeld van een implementatie van de standaard.

5.3.3 Kan de standaard rekenen op voldoende draagvlak?

5.3.3.1 Staan de belangrijkste stakeholders vanuit de overheid voor deze standaard achter de adoptie van de standaard?

Ja, de standaard is vastgesteld in het MIDO, daar worden alle stakeholders vertegenwoordigd. Ook is er een positief advies vanuit de GDI werkgroep architectuur Gegevensuitwisseling.

5.3.3.2 Staan de overheidsorganisaties die worden geraakt door een verplichting van de standaard achter het verplichte gebruik van de standaard?

Ja, alle overheidsorganisaties, zoals o.a. de Kadaster, DUO en Logius hebben te maken met deze verplichting. Zie ook 5.3.3.1

5.3.3.3 Wordt de aangemelde versie van de standaard binnen het organisatorische werkingsgebied door meerdere Nederlandse overheidsorganisaties gebruikt?

Nee, de huidige versie (1.1.0) is vrij nieuw. Maar er zijn verschillende overheidsorganisaties die gebruik maken van versie 1.0 van NL Gov Assurance Profile for OAuth 2.0, zoals gemeente Den Haag, Kadaster, de Politie en Logius.

5.3.3.4 Wordt een vorige versie van de standaard binnen het organisatorische werkingsgebied door meerdere Nederlandse overheidsorganisaties gebruikt?

Ja, eerdere versies van de standaard (versie 1.0) worden nog gebruikt binnen de overheid door onder andere gemeente Den Haag, Kadaster, DUO en Logius.

5.3.3.5 Is de aangemelde versie backwards compatible met eerdere versies van de standaard?

Ja, de nieuwe versie (1.1.0) is volledig backward compatible is met versie 1.0. De comptabiliteit tussen de nieuwe en eerdere versie worden in de praktijk geborgd.

5.3.3.6 *Zijn er voldoende positieve signalen over toekomstige gebruik van de standaard door (semi-)overheidsorganisaties, het bedrijfsleven en burgers?*

Ja, er zijn positieve signalen over het toekomstige gebruik van de standaard door overheidspartijen. Deze signalen komen van organisaties die deelnemen aan de overleggen over het beheer en doorontwikkeling van de standaard zoals onder andere Kennisplatform API's, Kadaster, Federatief Datastelsel, Sociale Verzekeringsbank en VNG Realisatie (namens gemeenten). NL Gov assurance profile for OAuth 2.0 versie 1.1.0 wordt door deze organisaties (of delen van hun achterban) ook al toegepast. Ook de NL-wallet zal gebruik maken van OAuth gebaseerde standaarden.

5.4 Opname op de lijst bevordert adoptie

De experts komen tot de conclusie dat NL Gov Assurance Profile for OAuth 2.0 versie 1.1.0 voldoet aan het criterium 'Opname op de lijst bevordert adoptie'.

NL Gov Assurance Profile for OAuth 2.0 is een incrementele update ten opzichte van de vorige versie (v1.0.0). Er zijn delen van de oorspronkelijke standaard (versie 1.0.0) deprecated (verouderd) verklaard, ook worden delen (niet meer) onvoldoende ondersteund. Er worden in de oorspronkelijke standaard (versie 1.0.0) vier flows benoemd waarvan twee als deprecated zijn verklaard.

NL Gov Assurance Profile for OAuth 2.0 is als geheel een breed gereedschapskist. De standaard voegt extra securitymaatregelen en andere features toe en daar waar nodig wijkt de standaard af van het bovenliggend profiel om de implementaties van OAuth binnen de rijksoverheid te stimuleren. Daar waar Nederlandse organisaties op een aantal regels vastlopen, biedt het NL Gov profiel een uitweg. Dit zou de adoptie van OAuth als geheel moeten bevorderen. De plaatsing op de lijst open standaarden met de status 'Pas toe of leg uit' biedt overheden houvast en een duidelijk signaal dat NL Gov Assurance Profile for OAuth 2.0 versie 1.1.0 de te verkiezen standaard is.

6 Adviezen bij opname van de standaard

De experts geven het Forum Standaardisatie volgende adviezen bij plaatsing van NL Gov Assurance Profile for OAuth 2.0 versie 1.1.0 op de 'Pas toe of leg uit'-lijst:

- De experts adviseren beheerder Logius om het Forum Standaardisatie op de hoogte te houden van eventuele veranderingen in het beheerproces van de standaard.
- De experts adviseren het Forum om de ontwikkelingen rondom een nieuwe versie van de standaard (versie 2.1) die in ontwikkeling is in de gaten te houden.