notitie

FORUM STANDAARDISATIE 6 MEI 2020
Agendapunt 3B - Forumadvies NL GOV profiel OAuth 2.0

Nummer:	FS-20200506.3B
Aan:	Forum Standaardisatie
Van:	Stuurgroep Open Standaarden
Datum:	10 april 2020
Versie:	1.0
Bijlagen:	Expertadvies OAuth 2.0 Reacties uit de consultatieronde OAuth 2.0 Forumadvies OAuth 2.0

1. Aanleiding en achtergrond

OAuth 2.0 is een open standaard voor de beveiliging van applicaties die gegevens uitwisselen met behulp van REST API's. 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.

OAuth 2.0 is een generieke standaard die meestal een nog aanvullend profiel vereist voor de toepassing in specifieke domeinen. Zo'n profiel is een verzameling aanvullende afspraken over het gebruik van OAuth 2.0 en kan gezien worden als een 'standaard op een standaard'.

Forum Standaardisatie heeft de standaard OAuth 2.0 in 2016 getoetst voor opname op de 'pas toe of leg uit'-lijst, waarbij een volledig expertonderzoek is uitgevoerd en het expertadvies ter openbare consultatie is aangeboden. Het resulterende Forumadvies OAuth 2.0 van april 2017 luidde dat eerst een Nederlands overheidsprofiel moet worden ontwikkeld voordat OAuth kan worden opgenomen op de 'pas toe of leg uit'-lijst.

In de periode tussen november 2017 en juli 2019 heeft het Kennisplatform APIs gewerkt aan een Nederlands overheidsprofiel voor OAUth 2.0, dat op 15 juli 2019 werd gepubliceerd als '*NL GOV Assurance profile for OAuth 2.0*'.

NL GOV Assurance profile for OAuth 2.0 bevat bindende afspraken over het gebruik van OAuth bij de Nederlandse overheid en moet beheerd worden volgens de criteria voor open standaarden. Daarom moet dit profiel gezien worden als een standaard op zichzelf en heeft het een korte toetsingsprocedure doorlopen waarvan een openbare consultatie het voornaamste deel uitmaakte.

Dit document bevat het Forumadvies voor de standaard *NL GOV Assurance profile for OAuth 2.0* en de onderliggende standaard OAUth 2.0.

2. Betrokkenen en proces

Om te komen tot dit Forumadvies is een verlengde toetsingsprocedure uitgevoerd. Deze bestond uit drie delen:

1. In 2016 is voor de standaard OAuth 2.0 de gebruikelijke toetsingsprocedure uitgevoerd. Deze bestond uit een expertonderzoek, een openbare consultatie en een Forumadvies. Het

Forumadvies stelde dat OAuth 2.0 voldoet aan de criteria om op de 'pas toe of leg uit'-lijst geplaatst te worden, mits er eerst een toepassingsprofiel wordt gespecificeerd voor de Nederlandse overheid.

2. Het Kennisplatform APIs heeft tussen november 2017 en juli 2019 gewerkt aan het *NL GOV Assurance profile for OAuth 2.0*. Dit gebeurde in een open proces waarvan een openbare technische consultatie deel uitmaakte.

3. Het advies om *NL GOV Assurance profile for OAuth 2.0* op de 'pas toe of leg uit' lijst op te nemen en OAuth 2.0 op de lijst aanbevolen standaarden is ter open consultatie is aangeboden op internetconsultatie.nl. Op basis van de reacties uit deze openbare consultatie en alle voorgaande stappen is dit Forumadvies opgesteld.

Paragraaf 5.2 geeft details over de stappen die in deze toetsingsprocedure werden uitgevoerd.

Bij de specificatie van *NL GOV Assurance profile for OAuth 2.0* was een brede groep belanghebbenden betrokken, waaronder Geonovum, Logius, gemeente Den Haag, Kadaster, RvIG, Rijkswaterstaat, Kennisnet, DUO, Justid, de Waarderingskamer, de gemeente Haarlem, Rijkswaterstaat, het ministerie van Binnenlandse Zaken en Koninkrijksrelaties, het ministerie van Economische Zaken en Klimaat en Enable-U.

3. Consequenties en vervolgstappen

Het Forum Standaardisatie brengt op basis van dit Forumadvies een advies uit aan het Overheidsbreed Beleidsoverleg Digitale Overheid. Het Overheidsbreed Beleidsoverleg Digitale Overheid bepaalt uiteindelijk op basis van het advies of NL GOV Assurance profile for OAuth2.0 op de lijst met open standaarden wordt opgenomen met als status 'pas toe of leg uit'.

Tegelijk met de *NL GOV Assurance profile for OAuth 2.0* heeft het Kennisplatform API's ook de standaard REST API Resign Rules aangemeld voor plaatsing op de 'pas toe of leg uit'-lijst. Kennisplatform API's heeft de twee standaarden *REST API Design Rules* en *NL GOV Assurance profile for OAuth 2.0* tegelijk met elkaar ontwikkeld waardoor de twee standaarden een sterk verband hebben. Hoewel de huidige versie van *REST API Design Rules* niet verwijst naar *NL GOV Assurance profile for OAuth 2.0,* heeft Kennisplatform APIs daarnaast REST API Design Rules Extensions gespecificeerd die wel refereren naar OAuth 2.0 met *NL GOV Assurance profile for OAuth 2.0* als verplichte veiligheidstandaard. Het ligt in de verwachting dat een deel van de *REST API Design Rules Extensions* —waaronder de referentie naar OAuth 2.0 met *NL GOV Assurance profile for OAuth 2.0*— in de toekomst deel gaat uitmaken van de *REST API Design Rules*.

4. Gevraagd besluit

Het Forum Standaardisatie wordt gevraagd om in te stemmen met onderstaand advies.

Het Forum Standaardisatie adviseert het Overheidsbreed Beleidsoverleg Digitale Overheid (OBDO) om:

1. *De standaard NL GOV Assurance Profile for OAuth 2.0 op te nemen op de 'pas toe of leg uit'-lijst.*
2. *De onderliggende standaard OAuth 2.0 op te nemen op de lijst aanbevolen standaarden.*
3. *Het functioneel toepassingsgebied voor NL GOV Assurance Profile for OAuth 2.0 als volgt vast te stellen: "NL GOV Assurance Profile for OAuth 2.0 moet worden toegepast bij 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 waarvoor ze recht van toegang hebben."*

5. Toelichting

5.1 Over de standaard

OAuth 2.0 is een autorisatiestandaard voor web applicaties die gegevens uitwisselen met behulp van REST API's. OAuth 2.0 maakt gebruik van 'tokens' waardoor vertrouwelijke gegevens als een gebruikersnaam of wachtwoord niet afgegeven hoeven te worden. Een 'token' geeft slechts toegang tot specifieke gegevens van één gebruikersaccount voor een bepaalde duur. Het expertadvies OAuth 2.0 van februari 2017 geeft meer details over de werking van OAuth.

NL GOV Assurance profile for OAuth 2.0 is een profiel op OAuth 2.0 dat nadere afspraken vastlegt over het gebruik van OAuth. Zo legt *NL GOV Assurance profile for OAuth 2.0* afspraken vast over hoe applicaties zich bij elkaar moeten registreren en hoe autorisatiecodes veilig uitgewisseld moeten worden. OAuth 2.0 laat daarin namelijk nog verschillende implementaties vrij.

Deze afspraken zijn specifiek voor het gebruik van OAuth 2.0 bij REST API's van de Nederlandse overheid. Wel baseert *NL GOV Assurance profile for OAuth 2.0* zich op internationale OAuth 2.0 profielen.

5.2 Hoe is het proces verlopen?

Om te komen tot dit Forumadvies is een uitgebreide en verlengde toetsingsprocedure uitgevoerd. Het eerste deel hiervan bestond uit de reguliere toetsingsprocedure voor OAuth 2.0 die in 2016 plaatsvond:

- Forum Standaardisatie besloot in de vergadering van 15 maart 2016 om OAuth 2.0 in behandeling te nemen voor plaatsing op de 'pas toe of leg uit'-lijst.
- Op 7 juli en 22 september 2016 kwam een groep experts bijeen om OAuth te toetsen op de criteria voor plaatsing op de 'pas toe of leg uit'-lijst en het functioneel toepassingsgebied vast te stellen. Op basis hiervan is een expertadvies samengesteld.
- Van 24 februari tot 25 maart 2017 is het expertadvies voor publieke consultatie aangeboden. Dit heeft drie reacties opgeleverd.
- Op basis van het expertadvies en de reacties uit de openbare consultatie heeft de procedurebegeleider een Forumadvies voor OAuth 2.0 opgesteld. De conclusie was dat OAuth voldoet aan de criteria om opgenomen te worden op de 'pas toe of leg uit'-lijst mits er eerst een toepassingsprofiel wordt gespecificeerd voor de Nederlandse overheid.

Het tweede deel bestond uit de specificatie en toetsing van *NL GOV Assurance profile for OAuth 2.0*, het Nederlands overheidsprofiel voor OAuth 2.0:

- In de loop van 2018 heeft het Kennisplatform APIs een Nederlands overheidsprofiel voor OAUth 2.0 gespecificeerd. Bij de specificatie van dit profiel voor de Nederlandse overheid was een brede groep belanghebbenden betrokken waaronder Logius, Geonovum, DUO, Gemeente Den Haag, Kadaster, RvIG, Rijkswaterstaat, Kennisnet, Gemeente Haarlem, Wetterskip Fryslan en Enable-U.
- Het Kennisplatform APIs heeft het Nederlands overheidsprofiel voor OAuth 2.0 ter openbare technische consultatie aangeboden van 13 februari tot 27 maart 2019. Hierop zijn tientallen reacties ontvangen die openbaar vastgelegd zijn op Github.
- Op basis van de ontvangen reacties heeft het Kennisplatform APIs het profiel gereviseerd, en op 15 juli 2019 formeel gepubliceerd onder de naam *NL GOV Assurance profile for OAuth 2.0*

Het derde deel bestond uit een openbare consultatie van het advies om *NL GOV Assurance profile for OAuth 2.0* op de 'pas toe of leg uit' lijst op te nemen en OAuth 2.0 op de lijst aanbevolen standaarden. Deze openbare consultatie liep van 21 februari tot en met 20 maart 2020 op Internetconsultatie.nl. Een tiental organisaties heeft gereageerd op deze openbare consultatie. Het commentaar van deze organisaties is weergegeven in paragraaf 5.4. Dit Forumadvies is gebaseerd op de informatie uit alle voorgaande stappen.

Merk op dat er in feite twee toetsingsprocedures zijn uitgevoerd: één voor OAuth 2.0 en één voor *NL GOV Assurance profile for OAuth 2.0,* waarbij de openbare consultatie van *NL GOV Assurance profile for OAuth 2.0* door het Kennisplatform APIs en de aansluitende revisie van de standaard het expertonderzoek verving.

5.3 Hoe scoort de standaard op de toetsingscriteria?

Open standaardisatieproces

NL GOV Assurance profile for OAuth 2.0 is ontwikkeld door het Kennisplatform APIs. Dit is een open samenwerkingsverband waar belanghebbenden zich zonder voorwaarden kosteloos bij kunnen aansluiten. De specificatie van de standaard wordt op het open platform GitHub beheerd, en is daardoor vrij toegankelijk voor alle geïnteresseerden. De specificatie zelf is onder Creative

Commons Attribution 4.0 International Public License (CC-BY) licentie gepubliceerd. Het Kennisplatform APIs heeft het *NL GOV Assurance profile for OAuth 2.0* van 13 februari tot en met 27 maart 2019 ter openbare consultatie aangeboden.

Eind 2019 heeft de Programmaraad Logius bepaald dat Logius het *NL GOV Assurance profile for OAuth 2.0* in beheer neemt mits het een plaats op de 'pas toe of leg uit' lijst van het Forum Standaardisatie krijgt. Logius brengt het beheer van *NL GOV Assurance profile for OAuth 2.0* onder in hetzelfde beheerproces als Digikoppeling, waarvoor Logius het predicaat 'Uitstekend Beheer' van het Forum Standaardisatie heeft.

De onderliggende standaard OAuth 2.0 wordt beheerd door IETF in een open standaardisatieproces.

Toegevoegde waarde

OAuth 2.0 is een veel toegepaste open autorisatiestandaard. OAuth 2.0 zorgt ervoor dat een aanbieder van een online dienst z'n gebruikers toegang kan geven aan online diensten van derden zonder persoonlijke gegevens zoals gebruikersnaam en wachtwoord aan de gebruiker te hoeven vragen en bewaren. Daarmee neemt het risico van misbruik van identiteitsgegevens af. Dienstverleners zoals Google en Facebook passen OAuth 2.0 op grote schaal toe.

IETF noemt OAuth 2.0 een '*autorization framework*' omdat het een generieke, open standaard is met veel opties, die veel verschillende implementaties toelaat. Daarom wordt OAuth 2.0 meestal gebruikt met aanvullende *profielen*: specifiekere afspraken over de configuratie van OAuth 2.0 voor een bepaald toepassingsdomein.

In het Forumadvies OAuth 2.0 van april 2017 onderkende Forum Standaardisatie de noodzaak om een profiel te specificeren voor de toepassing van OAuth 2.0 op API's van de Nederlandse overheid. *NL GOV Assurance profile for OAuth 2.0* voorziet in deze behoefte.

In het Forumadvies OAuth 2.0 was een functioneel toepassingsgebied vastgesteld. Aangepast naar de standaardsyntaxis die Forum Standaardisatie sinds 2017 hanteert, luidt het geadviseerde functioneel toepassingsgebied voor *NL GOV Assurance profile for OAuth 2.0*:

> *"NL GOV Assurance Profile for OAuth 2.0 moet worden toegepast bij 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 waarvoor ze recht van toegang hebben."*

Dit functioneel toepassingsgebied stelt impliciet dat *NL GOV Assurance Profile for OAuth 2.0* wordt gebruikt als profiel op OAuth 2.0.

Draagvlak

Het Forumadvies OAuth 2.0 van april 2017 stelt vast dat er voldoende draagvlak bestaat voor de verplichting van OAuth 2.0 voor de beveiliging van REST API's.

Aan de specificatie van *NL GOV Assurance profile for OAuth 2.0* heeft een brede groep overheidsorganisaties bijgedragen waaronder Logius, Geonovum, DUO, Gemeente Den Haag, Kadaster, RvIG, Rijkswaterstaat, Kennisnet, Gemeente Haarlem, Wetterskip Fryslan en Enable-U. Tijdens de technische openbare consultatie van *NL GOV Assurance profile for OAuth 2.0* ontving het Kennisplatform APIs overwegend positief commentaar van een tiental organisaties waaronder DUO, Justid, de Waarderingskamer, het ministerie van Binnenlandse Zaken en Koninkrijksrelaties en het ministerie van Economische Zaken en Klimaat. De technische feedback van deze organisaties heeft bijgedragen tot verdere aanscherping van de specificatie.

Tenslotte liet ook de expertbijeenkomst voor de REST API Design Rules in januari 2020 zien dat er breed draagvlak bestaat voor OAuth 2.0 en *NL GOV Assurance profile for OAuth 2.0* als verplicht onderdeel van REST API design regels (zie ook hoofdstuk 3 van dit Forumadvies).

Opname bevordert de adoptie

De laatste jaren neemt het gebruik van API's bij de overheid snel toe. Dit is onder andere te zien in initiatieven zoals Common Ground en Haal Centraal, en op https://developer.overheid.nl/. In deze fase is het belangrijk dat de overheid API's op een consistente, uniforme manier aanbiedt en er geen wildgroei ontstaat.

In het Forumadvies OAuth 2.0 van april 2017 stelde Forum Standaardisatie vast dat een 'pas toe of leg uit'- verplichting op zijn plaats is voor OAuth 2.0, mits er een profiel beschikbaar is voor de Nederlandse overheid. *NL GOV Assurance profile for OAuth 2.0* voorziet in deze voorwaarde.

5.4 Wat is de conclusie van de expertgroep en de consultatie?

Conclusie van het expertonderzoek

Het expertadvies OAuth 2.0 concludeert dat OAuth 2.0 voldoet aan de vier criteria voor opname op de lijst open standaarden van het Forum Standaardisatie, maar adviseert om eerst een toepassingsprofiel te specificeren voor de Nederlandse overheid. Dat profiel is nu beschikbaar.

Forum Standaardisatie heeft geen apart expertonderzoek laten doen voor *NL GOV Assurance profile for OAuth 2.0* omdat het Kennisplatform APIs deze taak feitelijk uitgevoerd heeft. Het commentaar op de standaard is daarbij gedocumenteerd op Github. Tevens is *NL GOV Assurance profile for OAuth 2.0* besproken in de expertbijeenkomst voor de REST API Design Rules op 30 januari 2020. De overwegingen van het Kennisplatform APIs en de discussies in de expertbijeenkomst voor de REST API Design Rules staan gedocumenteerd in paragraaf 5.3 hierboven. Hieruit volgt de conclusie dat *NL GOV Assurance profile for OAuth 2.0* voldoet aan de criteria voor opname op de 'pas toe of leg uit'-lijst.

Analyse van reacties uit de openbare consultatie

OAuth 2.0 is van 24 februari tot 25 maart 2017 aangeboden ter openbare consultatie. De (overwegend positieve) reacties uit deze consultatie staan met duiding beschreven in het Forumadvies OAuth van april 2017.

NL GOV Assurance profile for OAuth 2.0 is van 21 februari tot en met 20 maart 2020 ter openbare consultatie aangeboden op internetconsultatie.nl. In deze openbare consultatie werden 10 reacties ontvangen van de gemeente Den Haag, Kamer van Koophandel, Rijkswaterstaat, MedMij, DICTU, Unie van Waterschappen, Rijksdienst voor het Wegverkeer, Ministerie van Infrastructuur en Waterstaat, Piratenpartij Nederland en een particulier.

Alle bovengenoemde organisaties behalve de Piratenpartij Nederland onderschrijven het advies om *NL GOV Assurance profile for OAuth 2.0* op de 'pas-toe-of-leg-uit'-lijst te plaatsen. Hieronder bespreken wij het specifieke commentaar van iedere organisatie:

- **Kamer van Koophandel**: "De KVK vindt het belangrijk dat de afhankelijkheid van het OAUTH Profiel/OAUTH 2.0 standaard met OIDC wordt gelegd (want OIDC kun je niet gebruiken zonder OAuth)." *Aantekening: Forum Standaardisatie dankt de KvK neemt dit mee als OIDC wordt aangemeld voor de lijst open standaarden.*
- **Gemeente Den Haag**: "Wat betreft REST API Design Rules en Oauth, met beide standaarden wordt in Den Haag reeds gewerkt. Onze afdeling Architectuur, Security en Audit heeft geen bezwaar tegen het plaatsen van deze standaarden op de 'pas toe of leg uit'-lijst. Verdere input wordt nu niet verwacht, maar de afdeling is bekend met de websites forumstandaardisatie.nl en internetconsultatie.nl en zal in voorkomende gevallen via die weg haar eventuele input leveren." *Aantekening: Forum Standaardisatie dankt GEMEENTE DEN HAAG en neemt dit voor kennisgeving aan.*
- **Rijkswaterstaat**: "OAuth is een moderne authenticatie standaard die we vanuit IAM van harte ondersteunen m.b.t. opname als standaard." *Aantekening: Forum Standaardisatie dankt Rijkswaterstaat en neemt dit voor kennisgeving aan.*
- **MedMij**: "Op dit moment is OAuth (uiteraard!) ook verplicht opgenomen in het MedMij Afsprakenstelsel. Plaatsing op de lijst van standaarden betekent dat wij zorgaanbieders die gegevens aan hun patiënten beschikbaar stellen (zoals dat hoort volgens de AVG) beter kunnen uitleggen waarom binnen MedMij voor OAuth gekozen is. Gezondheidszorg is/kan daarom een belangrijke doelgroep voor jullie zijn. Maar die nergens/niet genoemd is. Tenslotte zorgt dit voor veiliger en betrouwbaarder gegevensuitwisseling, ook voor de patiënten in Nederland!" *Aantekening: Forum Standaardisatie dankt MedMij en onderschrijft het belang van APIs en OAuth voor de zorgsector. In het Forumadvies worden geen specifieke sectoren genoemd, maar de feedback van MedMij wordt meegenomen wanneer praktijkvoorbeelden worden geïnventariseerd.*

- **DICTU**: "Het bij deze aanvraag toegevoegde expert advies heeft betrekking op de eerdere aanvraag. Toen werd gevraagd om OAUTH op de 'pas toe of leg uit' lijst te plaatsen. In het expert advies is OAUTH getoetst tegen de criteria. Nu wordt gevraagd om het Nederlands Profiel op de 'pas toe of leg uit' lijst te plaatsen. Het wordt dus een zelfstandige standaard. Er is echter geen nieuw expert advies en er is dus geen toetsing van het Nederlands Profiel tegen de criteria van de lijst. Het profiel is opgesteld door kundige mensen, maar lijkt überhaupt niet door anderen getoetst te zijn (tenminste, het staat niet in het document). Is er bijvoorbeeld inspraak mogelijk bij volgende versies van het Nederlands Profiel; hoe is het beheer van deze standaard georganiseerd. Volgens mij behoort toetsing tegen de criteria plaats te vinden voordat het Nederlands Profiel op de 'pas toe of leg uit' lijst geplaatst wordt." *Aantekening: Forum Standaardisatie dankt DICTU en begrijpt de zorgen over het gevolgde proces. Zoals beschreven in paragrafen 5.2 en 5.3 hierboven zijn er in feite twee toetsingsprocedures uitgevoerd: één voor OAuth 2.0 en één voor NL GOV Assurance profile for OAuth 2.0.*
  In de toetsingsprocedure van NL GOV Assurance profile for OAuth 2.0 is het expertonderzoek vervangen door de openbare technische consultatie van NL GOV Assurance profile for OAuth 2.0 door het Kennisplatform APIs. Bij de specificatie van NL GOV Assurance profile for OAuth 2.0 was een groep experts betrokken van uiteenlopende overheidsorganisatie waaronder de Rijksoverheid, uitvoeringsorganisaties, gemeenten en een waterschap. Het specificatieproces stond bovendien open voor alle andere belanghebbenden. Om maximale terugkoppeling te krijgen heeft het Kennisplatform APIs de NL GOV Assurance profile for OAuth 2.0 begin 2019 ter openbare technische consultatie gepubliceerd en aangepast op basis van de ontvangen reacties.
  Aangezien bij de specificatie en technische consultatie al een kritieke massa van experts uit de breedte van de overheid betrokken waren, en alle belanghebbende de kans hebben gehad om bij te dragen, had het voor Forum Standaardisatie weinig meerwaarde om een aparte expertbijeenkomst te organiseren. De reacties op Github komen in de plaats van het expertadvies en paragraaf 5.3 van dit Forumadvies vat samen hoe NL GOV Assurance profile for OAuth 2.0 voldoet aan de vier criteria voor opname op de 'pas toe of leg uit'-lijst..
- **Unie van Waterschappen**: "Namens de Unie van Waterschappen en in overleg met Het Waterschapshuis deel ik u graag mede dat de waterschappen het voornemen onderschrijven." *Aantekening: Forum Standaardisatie dankt de Unie van Waterschappen en het Waterschapshuis en neemt dit voor kennisgeving aan.*

- **Rijksdienst voor het Wegverkeer**: "In lijn met de consultatie hechten wij veel waarde aan het op te stellen gemeenschappelijk toepassingsprofiel en bijbehorende randvoorwaarden. OAUTH kent nog veel implementatie vrijheid. Fouten kunnen leiden tot beveiligingsincidenten. Wij zien gedegen referentie implementaties als een goede aanvulling om dit risico te minimaliseren. Een substantieel onderdeel van de dienstverlening van RDW is informatieverstrekking. De 'pas toe of leg uit' lijst bevat al vele standaarden die hier mee te maken hebben. Zo ook OAUTH 2.0. Duidelijke richtlijnen omtrent de functionele toepassing van de verschillende standaarden en in welke context, zou een waardevolle toevoeging zijn. *Aantekening: Forum Standaardisatie dankt RDW en neemt de suggestie ter harte om de informatie over de samenhang van standaarden op de 'pas toe of leg uit'-lijst te verbeteren.*

- **Ministerie van Infrastructuur en Waterstaat**: "ILT is hierbij betrokken en is akkoord met deze standaard. DCI: ik ben voor OAuth als open standaard. Of het nodig is om daar een voor Nederland specifieke toevoeging over af te spreken kan ik niet goed beoordelen maar het levert hoe dan ook een heel nuttige discussie op, dus helemaal eens met het voorgestelde." *Aantekening: Forum Standaardisatie dankt het ministerie van Infrastructuur en Waterstaat (ILT en DCI) en neemt dit voor kennisgeving aan.*

- **Piratenpartij Nederland**: "Het idee achter OAuth is goed en heeft grote voordelen als het gaat over authenticatie. Er zitten echter ook valkuilen aan het gebruik van een externe authenticator. Zo bepleit het voorstel ten onrechte dat de implementatie van OAuth er voor zorgt dat privacy risico's, risico's op identiteitsdiefstal en misbruik van identiteitsgegevens afnemen. Deze risico's en misbruik hebben te maken met securityfouten in applicaties, zwakke wachtwoorden en het ontbreken van een degelijke 2FA en hebben niets te maken met welke methode er wordt gebruikt voor authenticatie. De acceptatie van OAuth zal samenhangen met het aantal partijen dat OAuth zal aanbieden en hun imago met betrekking tot privacy. Zeker ook omdat de OAuth-provider een profiel op kan bouwen van hoe en welke applicaties gebruikt worden. Mede om die

reden is het aan te raden om beheer en ontwikkeling te scheiden. Het beheer van een OAuth-omgeving behoort niet bij een commerciële partij, maar bij één onafhankelijke en transparante non-profit organisatie die wordt ondersteund door privacy voorvechters zoals de Piratenpartij en Bits of Freedom. Een slechte implementatie van OAuth 2.0 kan er nog steeds voor zorgen dat er via scripting kan worden aangemeld. Een goed securitybeleid is veel breder dan alleen een lijstje met te gebruiken methodieken. In zo'n securitybeleid zouden bijvoorbeeld standaarden met betrekking tot sessie-tijden en refresh-tokens kunnen worden opgenomen. Het gevaar ligt op de loer dat met het toevoegen van OAuth een vals gevoel van veiligheid wordt gecreëerd. Het voorstel impliceert dat OAuth 2.0 alleen gaat over user-authenticatie, maar dat is niet waar. OAuth 2.0 kan ook worden gebruikt voor server-server communicatie. De Piratenpartij zou graag een beslisboom zien over wanneer je wel of niet OAuth dient toe te passen. Voor simpele data-uitwisseling waarin geen privégegevens zitten (denk bijvoorbeeld aan GIS-data) is het overdreven om een Oauth-mechanisme in te richten. Het originele OAuth 2.0 (RFC 6749) stamt uit 2012 en is dus al acht jaar oud. De wereld verandert snel en dat geldt zeker voor authenticatie en autorisatie. Door nu OAuth 2.0 als standaard neer te leggen, wordt de weg van verbetering en innovatie nodeloos moeilijker gemaakt. Het toevoegen op de "pas toe of leg uit"-lijst is volgens de Piratenpartij dan ook niet de te volgen weg. Ja, OAuth is de way to go, maar niet door het om deze manier af te dwingen." *Aantekening: Forum Standaardisatie dankt de Piratenpartij voor de uitvoerige reactie. De Piratenpartij stelt dat toepassing van OAuth 2.0 geen veiligheid garandeert en dat OAuth 2.0 problemen met privacy kan veroorzaken als het beheer in verkeerde handen valt. Dit zijn gegronde argumenten en terechte zorgen. De standaard NL GOV Assurance profile for OAuth 2.0 (die de Piratenpartij niet noemt) heeft precies als doel om afspraken vast te leggen over het gebruik van OAuth 2.0 die veelvoorkomende configuratiefouten voorkomen en een veiliger gebruik van de standaard stimuleren. Natuurlijk geeft zelfs de combinatie van OAuth 2.0 met NL GOV Assurance profile for OAuth 2.0 geen waterdichte veiligheid. De Piratenpartij stelt terecht dat een veiligheidsbeleid breder is dan een lijst toe te passen standaarden. Dit is een kanttekening die we bij alle standaarden op de 'pas toe of leg uit'-lijst maken, met name Internet veiligheidstandaarden zoals TLS, SPF, DKIM, DMARC, DNSSEC en DANE. Forum Standaardisatie is zich hiervan bewust. Maar het risico dat organisaties uiteenlopende, incompatibele en leveranciersafhankelijke technologieën gaan gebruiken als NL GOV Assurance profile for OAuth 2.0* ***niet*** *wordt geplaatst op de 'pas toe of leg uit'-lijst, weegt hier zwaarder dan de kans dat organisaties een vals gevoel van veiligheid krijgen door de standaard* ***wel*** *te verplichten.*
Hetzelfde geldt voor argument dat standaardisatie innovatie beperkt. Het risico van wildgroei weegt zwaarder dan de kans dat NL GOV Assurance profile for OAuth 2.0 op de 'pas toe of leg uit'-lijst innovatie zou kunnen remmen.
De Piratenpartij stelt terecht dat commerciële partijen die OAuth 2.0 diensten aanbieden, misbruik kunnen maken van de (meta)data die daarbij verzameld kunnen worden. De overheid draagt verantwoordelijkheid voor ethisch en veilig gebruik van deze standaard. Zo zal de overheid bijvoorbeeld geen toegang tot haar APIs moeten geven op basis van accounts bij Google of Facebook, zoals dat wel gebruikelijk is bij veel commerciële diensten. De 'pas toe of leg uit'-lijst stelt geen bindende eisen aan verantwoord gebruik van een standaard maar kan wel verwijzen naar richtlijnen. Forum Standaardisatie bekijkt hoe dit aspect bij opname op de 'pas toe of leg uit'-lijst gedocumenteerd kan worden. Tenslotte vraagt de Piratenpartij om betere informatie (een beslisboom) over wanneer OAuth 2.0 toegepast moet worden. Het functioneel toepassingsgebied beperkt het verplichte gebruik van NL GOV Assurance profile for OAuth 2.0 tot client-server interacties bij het gebruik van REST APIs. Forum Standaardisatie bekijkt desondanks hoe de informatie over het gebruik van OAuth 2.0 verbeterd kan worden, mogelijk in de vorm van een beslisboom.

5.5 Welke additionele adviezen zijn er ten aanzien van de adoptie van de standaard?

In het expertadvies OAuth 2.0 roepen de experts op om:

> *"…regulier (bijvoorbeeld 2x per jaar) de afstemming te zoeken met de deelnemers van de expertgroep om enerzijds implementatieproblemen te voorkomen met betrekking tot het toepassingsprofiel en anderzijds kennis te delen over het gebruik van de standaard."*

Het Kennisplatform APIs neemt deze rol sinds 2018 op zich en brengt de experts en belanghebbenden meerdere keren per jaar bij elkaar om kennis en ervaring te delen over REST API Resign Rules, API Design Rules Extensions, OAuth 2.0 en het *NL GOV Assurance profile for OAuth 2.0*.

6. Referenties

[1] Expertadvies OAuth 2.0

[2] Reacties uit de consultatieronde OAuth 2.0

[3] Forumadvies OAuth 2.0

[4] Reacties uit de consultatieronde NL GOV Assurance profile for OAuth2.0

https://www.forumstandaardisatie.nl/sites/bfs/files/Commentaar-uit-de-openbare-consultatie-NLGOV-profile-OAuth2.0.pdf