Notitie

Aan: Forum Standaardisatie

Van: Bureau Forum Standaardisatie

Datum: 10 april 2020

Versie: 1.0

Betreft: Reacties uit de openbare consultatie NL GOV Profile for OAuth 2.0

Inleiding

Dit document bevat de reacties die tussen 21 februari en 20 maart 2020 werden ontvangen op de openbare consultatie voor plaatsing van NL GOV Profile for OAuth 2.0 op de lijst van aanbevolen standaarden van het Forum Standaardisatie. Tijdens de openbare consultatie zijn in totaal tien reacties binnen gekomen. Zeven reacties kwamen vanuit (semi) overheidspartijen, een reactie van een politieke partij en een reactie van een particulier. Een deel van de reacties zijn via mail binnengekomen en een deel via internetconsultatie.nl.

Reacties uit de openbare consultatie

Reactie van een particulier:

Naam: J.M. Beoletto
Emailadres: --
Plaats: --
Datum: 21 februari 2020 (10:19)

Vraag 1
Wilt u reageren op het advies van de experts om NL GOV Profile for OAuth2.0 op de 'pas toe of leg uit'-lijst te plaatsen (paragraaf 1 van het expertadvies)?
Denkt u nu echt dat de gemiddelde Nederlander ook maar iets begrijpt van deze braaktaal?

Reactie van Medmij

Naam: Medmij
Emailadres: --
Plaats: --
Datum: 27 februari 2020 (13:50)

Vraag 1
Onderschrijft u het voornemen van het Forum Standaardisatie om het Nederlands overheidsprofiel OAuth op de ‘pas toe of leg uit’ lijst te plaatsen, en OAuth 2.0 op de lijst aanbevolen standaarden te plaatsen? Indien uw antwoord ‘nee’ is, gaarne een onderbouwing van uw antwoord onder vraag 2.

Ja.

Vraag 2
Heeft u commentaar of suggesties met betrekking tot de plaatsing van het Nederlands overheidsprofiel OAuth op de 'pas toe of leg uit' en de plaatsing van OAuth 2.0 op de lijst aanbevolen standaarden?
Ja. 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!

Vraag 3
Heeft u verder nog opmerkingen die verband houden met de plaatsing van het Nederlands overheidsprofiel OAuth op de 'pas toe of leg uit' en de plaatsing van OAuth 2.0 op de lijst aanbevolen standaarden?
Nee, ik laat geheel bij jullie of bovenstaande suggestie betekenis vol kan zijn.
Ik wens jullie veel succes en steun jullie van harte.

Reactie van Dictu:

Naam: DICTU
Emailadres: --
Plaats: --
Datum: 28 februari 2020 (15:21)

Vraag 1
Onderschrijft u het voornemen van het Forum Standaardisatie om het Nederlands overheidsprofiel OAuth op de 'pas toe of leg uit' lijst te plaatsen, en OAuth 2.0 op de lijst aanbevolen standaarden te plaatsen? Indien uw antwoord 'nee' is, gaarne een onderbouwing van uw antwoord onder vraag 2.
Ja, maar wel met een opmerking, zie vraag 2.

Vraag 2
Heeft u commentaar of suggesties met betrekking tot de plaatsing van het Nederlands overheidsprofiel OAuth op de 'pas toe of leg uit' en de plaatsing van OAuth 2.0 op de lijst aanbevolen standaarden?
Het bij deze aanvraag toegevoegde expert advies heeft betrekking op de eerdere aanvraag. Toen werd gevraagd om OAUTH op de 'pas to 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.

Vraag 3
Heeft u verder nog opmerkingen die verband houden met de plaatsing van het Nederlands overheidsprofiel OAuth op de 'pas toe of leg uit' en de plaatsing van OAuth 2.0 op de lijst aanbevolen standaarden?
Geen verdere opmerkingen

Reactie Unie van Waterschappen:

Naam: Unie van Waterschappen (mr. CM Contreras Leon - Dunnink)
Emailadres: --
Plaats: --
Datum: 19 maart 2020 (14:10)

Vraag 1
Onderschrijft u het voornemen van het Forum Standaardisatie om het Nederlands overheidsprofiel OAuth op de 'pas toe of leg uit' lijst te plaatsen, en OAuth 2.0 op de lijst aanbevolen standaarden te plaatsen? Indien uw antwoord 'nee' is, gaarne een onderbouwing van uw antwoord onder vraag 2.
Namens de Unie van Waterschappen en in overleg met Het Waterschapshuis deel ik u graag mede dat de waterschappen het voornemen onderschrijven.

Vraag 2
Heeft u commentaar of suggesties met betrekking tot de plaatsing van het Nederlands overheidsprofiel OAuth op de 'pas toe of leg uit' en de plaatsing van OAuth 2.0 op de lijst aanbevolen standaarden?
Het heeft de voorkeur van de waterschappen dat de standaarden op de PTLU lijst worden geplaatst.

Vraag 3
Heeft u verder nog opmerkingen die verband houden met de plaatsing van het Nederlands overheidsprofiel OAuth op de 'pas toe of leg uit' en de plaatsing van OAuth 2.0 op de lijst aanbevolen standaarden?
Nee

Reactie Dienst Wegverkeer (RDW):

Naam: RDW (M Peters)
Emailadres: --
Plaats: --
Datum: 20 maart 2020 (12:42)

Vraag 1
Onderschrijft u het voornemen van het Forum Standaardisatie om het Nederlands overheidsprofiel OAuth op de 'pas toe of leg uit' lijst te plaatsen, en OAuth 2.0 op de lijst aanbevolen standaarden te plaatsen? Indien uw antwoord 'nee' is, gaarne een onderbouwing van uw antwoord onder vraag 2.
Ja

Vraag 2
Heeft u commentaar of suggesties met betrekking tot de plaatsing van het Nederlands overheidsprofiel OAuth op de 'pas toe of leg uit' en de plaatsing van OAuth 2.0 op de lijst aanbevolen standaarden?
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.

Vraag 3
Heeft u verder nog opmerkingen die verband houden met de plaatsing van het Nederlands overheidsprofiel OAuth op de 'pas toe of leg uit' en de plaatsing van OAuth 2.0 op de lijst aanbevolen standaarden?
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.

Reactie van een politieke partij:

Naam: Piratenpartij Nederland (S de Boer)
Emailadres: --
Plaats: --
Datum: 20 maart 2020 (14:49)

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-proffit 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. Het gevaar ligt op de loer dat met het toevoegen van OAuth een vals gevoel van veiligheid wordt gecreëerd. 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.

Reactie van ministerie Infrastructuur en Waterstaat (-email)

Naam: C.T. (Chris) Breebaart
Emailadres: --
Plaats: --
Datum: 20 maart 2020

1. **Onderdeel: ILT**

Het advies om het Nederlands overheidsprofiel OAuth (een autorisatiestandaard voor met name webbased applicaties die gegevens uitwisselen met behulp van API's) op de 'pas toe of leg uit'-lijst te plaatsen conform het Forumadvies van 2017. En om de onderliggende standaard OAuth op de lijst aanbevolen standaarden te plaatsen. ILT is hierbij betrokken en is akkoord met deze standaard.

2. **Onderdeel: DCI**

OAuth: 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.

3. **Onderdeel: RWS**

oAuth is een moderne authenticatie standaard die we vanuit IAM van harte ondersteunen mbt opname als standaard.

Reactie van Kamer van Koophandel (KvK) (–email)

Naam: Frits Maas ICT Architect Kamer van Koophandel
Emailadres: --
Plaats: --
Datum: 20 maart 2020

Vraag 1 van 3

Onderschrijft u het voornemen van het Forum Standaardisatie om het Nederlands overheidsprofiel OAuth op de 'pas toe of leg uit' lijst te plaatsen, en OAuth 2.0 op de lijst aanbevolen standaarden te plaatsen? Indien uw antwoord 'nee' is, gaarne een onderbouwing van uw antwoord onder vraag 2. **Ja**

Vraag 3 van 3

Heeft u verder nog opmerkingen die verband houden met de plaatsing van het Nederlands overheidsprofiel OAuth op de 'pas toe of leg uit' en de plaatsing van OAuth 2.0 op de lijst aanbevolen standaarden?

Ja; 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).

Reactie van VNG Adviescommissie Archieven (-email)

Naam: Jamil Jawad
Emailadres: --
Plaats: --
Datum: 20 maart 2020

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.