Forum Standaardisatie

Expertadvies OAuth 2.0

Ter openbare consultatie

Datum 24 februari 2017

Colofon

Projectnaam	Expertadvies OAuth 2.0
Versienummer	1.0
Locatie	Den Haag
Organisatie	Forum Standaardisatie Postbus 96810 2509 JE Den Haag forumstandaardisatie@logius.nl
Auteur	Paul Dam
Onafhankelijk voorzitter	Roy Tomeij

Inhoud

Forumadvies & Managementsamenvatting

Advies aan het Forum
De expertgroep adviseert het Forum Standaardisatie om eerst een overheidstoepassingsprofiel voor de standaard OAuth 2.0 op te stellen voordat de standaard opgenomen wordt op de lijst met open standaarden voor de status 'pas toe of leg uit'. (zie de adviezen hieronder).

Als functioneel toepassingsgebied wordt voorgesteld:

Het gebruik van OAuth 2.0 is verplicht voor applicaties waarbij gebruikers (resource owner) toestemming geven (impliciet of expliciet) aan een dienst (van een derde) om namens hem toegang te krijgen tot specifieke gegevens via een RESTful API.

Het gaat dan om een RESTful API waar de resource owner recht tot toegang heeft.

Als organisatorisch werkingsgebied wordt geadviseerd:

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

Waar gaat het inhoudelijk over?
Met OAuth 2.0 kunnen gebruikers of organisaties een programma of website toegang geven tot specifieke (privé)gegevens, die opgeslagen zijn op een ander systeem, zonder hun gebruikersnaam en wachtwoord uit handen te geven. OAuth 2.0 is een autorisatiestandaard voor met name webbased applicaties die gegevens uitwisselen met behulp van API's. OAuth 2.0 maakt gebruik van tokens, waardoor vertrouwelijke gegevens als een gebruikersnaam of wachtwoord niet afgegeven hoeven te worden. Elk token geeft slechts toegang tot specifieke gegevens van één website voor een bepaalde duur.

Het is voor telefoons, tablets, wearables, en internet of things apparaten een vaak gebruikte beveiligingsstandaard. Een bekend voorbeeld voor gebruikers is de mogelijkheid om bij een bepaalde onlinedienst in te loggen gebruikmakend van een Google-account of Facebook-account. Dit wordt ondersteund door de OAuth 2.0-standaard.

Hoe is het proces verlopen?
Om tot dit advies te komen is op 7 juli en 22 september 2016 een expertgroep bijeengekomen om over het toepassings- en werkingsgebied van OAuth 2.0 te discussiëren en om de standaard te toetsen aan de toetsingscriteria. Dit expertadvies vat de uitkomsten van de discussie en toetsing samen.

Hoe scoort de standaard op de toetsingscriteria?

Toegevoegde waarde
Met de standaard is mogelijk dat aanbieders van onlinediensten geen (gevoelige) inloggegevens van gebruikers hoeven te vragen en te bewaren om gebruik te maken van andere onlinediensten en gegevens waar deze gebruiker toegang toe heeft. Daarmee nemen privacyrisico's en risico's op identiteitsdiefstal en misbruik van identiteitsgegevens af. Het belang van de standaard neemt toe omdat online diensten steeds meer

via het web met behulp van API's met elkaar communiceren, met name in de commerciële wereld, maar ook in toenemende mate binnen de overheid.

Het probleem is echter dat zonder vastgesteld toepassingsprofiel de interoperabiliteit binnen de overheid (en eventueel daarbuiten) niet geborgd is. Iedereen zal dan zijn eigen implementantie verzorgen, wat de beoogde interoperabiliteit niet ten goede komt.

Open standaardisatieproces
De expertgroep concludeert dat het standaardisatieproces van IETF voldoende open is. OAuth 2.0 is een internationale standaard waarbij de Nederlandse overheid haar belang niet direct heeft geborgd. De experts zijn van mening dat dat vanwege het feit dat het hier om een internationale standaard gaat ook niet noodzakelijk is. Ondanks deze (geringe) beperkingen concludeert de expertgroep dat het standaardisatieproces van IETF voldoende open is.

Het standaardisatieproces voldoet aan alle hoofdcriteria, maar niet aan enkele grijs-gearceerde criteria. Het beheer van de standaard voldoet daardoor niet aan de criteria voor 'uitstekend beheerproces'.

Draagvlak
De expertgroep concludeert dat het draagvlak voor OAuth 2.0 voldoende is. Hoewel de standaard nog niet door veel overheidsorganisaties wordt gebruikt, zijn er voldoende signalen dat dit in de toekomst zal toenemen. Toekomstige gebruikers kunnen hierbij rekenen op voldoende ondersteuning, in de vorm van expertise bij marktpartijen en implementaties in software, voor de implementatie en bij het gebruik van de standaard.

Opname bevordert de adoptie
De expertgroep concludeert dat de 'pas toe of leg uit'-lijst het passende middel is om de adoptie van de standaard binnen de (semi)overheid te bevorderen maar wel pas nadat er een gemeenschappelijk toepassingsprofiel is ontwikkeld.

Welke additionele adoptieadviezen of vervolgactiviteiten zijn er ten aanzien van de standaard?
Aanbevolen wordt om de experts van deze experttoets tezamen met de volgende potentiële gebruikers van de standaard binnen de overheid een toepassingsprofiel te laten opstellen:
- Logius (als beheerder van DigiD, eHerkenning en Idensys),
- Ministerie van EZ (als verantwoordelijke eIDAS-verordening) en
- Rijksdienst voor Identiteitsgegevens.

Daarmee kunnen variaties in de implementatie worden voorkomen en wordt de interoperabiliteit geborgd. De experts hebben daartoe reeds een aantal te hanteren uitgangspunten in de expertbijeenkomst met elkaar afgestemd, zie vervolgadvies. Het Forum Standaardisatie zou hierbij in eerste instantie de rol van secretariaat op zich moeten nemen.

Vervolgens wordt aanbevolen 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.

1 Doelstelling expertadvies

1.1 Achtergrond

Het gebruik van open standaarden en het voorkomen van vendor lock-in is een van de doelstellingen van de Nederlandse overheid. Dit beleid wordt herbevestigd in actieplan "Open overheid", de digitale agenda 2011-2015, de digitale agenda 2017 en de kabinetsreactie op het rapport Elias. Deze plannen onderstrepen de noodzaak van het zoveel mogelijk meenemen van open standaarden bij het ontwerpen van informatiesystemen.

Een van de maatregelen om de adoptie van standaarden te bevorderen is het beheren van een lijst met standaarden, die vallen onder het principe 'pas toe of leg uit'. Het Nationaal Beraad Digitale Overheid spreekt zich uit over de standaarden die op de lijst zullen worden opgenomen, o.a. op basis van een expertbeoordeling van de standaard. Het Nationaal Beraad wordt geadviseerd door het Forum Standaardisatie. Het Bureau Forum Standaardisatie ondersteunt beide instellingen.

1.2 Doelstelling expertadvies

Onderwerp van dit expertadvies is de standaard OAuth 2.0. Doel van dit advies is om, aan de hand van de toetsingscriteria van het Forum Standaardisatie vast te stellen of OAuth 2.0 moet worden opgenomen op de 'pas toe of leg uit'-lijst, al dan niet onder bepaalde voorwaarden.

1.3 Doorlopen proces

Het Forum Standaardisatie heeft besloten de standaarden OAuth 2.0 en OpenID Connect in procedure te nemen voor opname op de 'pas toe of leg uit'-lijst. Aanleiding daartoe was de bespreking door het Forum van het Discussiedocument RESTful API's.[1]

Voor het opstellen van dit advies is de volgende procedure doorlopen:

- op basis van het besluit OAuth 2.0 en OpenID Connect in procedure te nemen is een expertgroep samengesteld en een voorzitter aangesteld. Voor de experts is een voorbereidingsdossier opgesteld.
- de expertgroep is op 7 juli en op 22 september 2016 bijeengekomen om de standaarden, de aandachtspunten en openstaande vragen uit het voorbereidingsdossier te bespreken. Daarbij is vastgesteld dat OpenID Connect niet voor opneming op de lijst open standaarden in aanmerking komt. Tijdens de bijeenkomst is ook het advies ten aanzien van het functioneel toepassingsgebied voor OAuth 2.0 vastgesteld.

De uitkomsten van de expertgroep zijn door de voorzitter en begeleider verwerkt in dit adviesrapport. Een eerste conceptversie is aan de leden van de expertgroep gestuurd met het verzoek om een reactie. Na verwerking van deze reacties is het rapport afgerond en gereed voor openbare consultatie.

---

1 Zie de vergaderstukken van het Forum Standaardisatie onder https://www.logius.nl/fileadmin/os/Vergaderstukken/FS_160315.4A_Discussie_document_RESTful_APIs_versie_1.0.pdf).

1.4 Vervolg

Het expertadvies zal ten behoeve van een publieke consultatie openbaar worden gemaakt door het Bureau Forum Standaardisatie. Eenieder kan gedurende de consultatieperiode op dit expertadvies zijn/haar reactie geven. De begeleider bundelt de reacties en verwerkt deze in samenspraak met de expertgroep in het expertadvies. Het Bureau Forum Standaardisatie legt vervolgens de gebundelde reacties en het (eventueel bijgestelde) advies voor aan het Forum Standaardisatie. Op voorhand adviseren de experts het Forum Standaardisatie om opdracht te geven voor het opstellen van een overheidstoepassingsprofiel voor OAuth 2.0, voordat OAuth 2.0 op de lijst open standaarden wordt geplaatst.

Het Forum Standaardisatie zal op basis van het expertadvies en relevante inzichten uit de openbare consultatie een advies aan het Nationaal Beraad opstellen. Het Nationaal Beraad bepaalt uiteindelijk op basis van het advies van het Forum of en zo ja, met welke status (‘pas toe of leg uit’ of ‘aanbevolen’) de standaard op lijst open standaarden komt.

1.5 Samenstelling expertgroep

Het Forum streeft naar een zo representatief mogelijke expertgroep, met een evenwichtige vertegenwoordiging van (toekomstige) gebruikers (zowel publiek als privaat), leveranciers, wetenschappers en andere kennishebbers. Daarnaast is een onafhankelijke voorzitter aangesteld om de expertgroep te leiden en als verantwoordelijke op te treden voor het uiteindelijke expertadvies.

De volgende vertegenwoordigers hebben deelgenomen aan de expertbijeenkomst:

- Joris Joosten, Logius,
- Kick Willemse, Evidos,
- Jeroen de Beer, Anoigo,
- Benoist Claassen, Digidentity,
- Gert Maneschijn, RDW,
- Joost van Dijk, SURFnet,
- Denis Joannides, Onegini,
- Remco Schaar, Logius,
- Mark Lagendijk, Connectis,
- Martijn Oostdijk, InnoValor,
- Jan Speksnijder, Kadaster,
- Erik de Jong, Traxion,
- H-P Köhler, Kennisnet,
- Frank Terpstra, Geonovum,
- André de Kok, Rijksdienst voor Identiteitsgegevens,
- Mark Dobrinic, Twobo Technologies,
- Yves Fonk, Ministerie van EZ/DICTU,
- René Bakker, Rijksdienst voor Ondernemend Nederland.

Roy Tomeij trad op als onafhankelijk voorzitter. Paul Dam, adviseur bij Verdonck, Klooster & Associates, begeleidde de expertgroep in opdracht van het Bureau Forum Standaardisatie. Lancelot Schellevis van het Bureau Forum Standaardisatie was als toehoorder bij de expertbijeenkomst aanwezig.

1.6 Leeswijzer

In hoofdstuk 2 wordt beschreven in welke gevallen de standaard functioneel gezien gebruikt zou moet worden (functioneel toepassingsgebied) en door welke organisaties deze gebruikt zou moeten worden (organisatorisch werkingsgebied). Om te bepalen of de standaard opgenomen moet worden op de lijst met standaarden voor ‘pas toe of leg uit’, is deze getoetst aan een viertal vastgestelde criteria. In hoofdstuk 3 staat het resultaat van deze toetsing.

2 Toepassings– en werkingsgebied

Van overheidsorganisaties wordt verwacht dat zij de lijst met open standaarden hanteren bij aanbestedingstrajecten volgens het 'pas toe of leg uit'-regime. Afhankelijk van de aan te schaffen functionaliteit zal bepaald moeten worden welke koppelvlakken geïmplementeerd moeten worden, en welke standaarden uit de lijst hiervoor ingezet dienen te worden. Om dit te kunnen doen heeft de expertgroep gekeken in welke gevallen de standaard functioneel gezien gebruikt zou moeten worden (functioneel toepassingsgebied), en door welke organisaties deze gebruikt zouden moeten worden (organisatorisch werkingsgebied).

2.1 Toelichting OAuth 2.0

Met OAuth 2.0 kunnen gebruikers een programma of website toegang geven tot hun privégegevens, die opgeslagen zijn op een ander systeem, zonder hun gebruikersnaam en wachtwoord uit handen te geven. OAuth 2.0 is een autorisatiestandaard voor met name webbased applicaties die gegevens uitwisselen met behulp van API's.

OAuth 2.0 maakt gebruik van tokens, waardoor vertrouwelijke gegevens als een gebruikersnaam of wachtwoord niet afgegeven hoeven te worden. Elk token geeft slechts toegang tot specifieke gegevens van één website voor een bepaalde duur. Het is voor telefoons, tablets, wearables, en internet of things apparaten een vaak gebruikte beveiligingsstandaard.

Onderstaande toont een typisch gebruiksscenario voor OAuth 2.0 (de figuur is niet bedoeld om een technische uitwerking te tonen van de werking van OAuth 2.0).

Figuur 1: Typisch gebruiksscenario voor OAuth 2.0.

OAuth 2.0 is gebaseerd op REST-principes en kent optionele keuzes en toevoegingen, zoals de mogelijkheid om identiteitsgegevens uit te wisselen en te versleutelen.

Voorbeeld: RESTful API's bij digitale ondersteuning Omgevingswet
Bij de digitale ondersteuning van de Omgevingswet wordt er vanuit gegaan dat de overheid API's zal gaan aanbieden aan de buitenwereld waar iedereen apps op mag ontwikkelen. Deze API's zullen op REST gebaseerd zijn en daar past OAuth 2.0 bij als authenticatie- en autorisatiemechanisme. SAML en OAuth 2.0 zullen in gezamenlijkheid gebruikt worden. Om de individuele gebruiker te identificeren wordt SAML gebruikt richting DigiD, eHerkenning en Idensys.

Het is gewenst dat de ontwikkelaars van apps en API's zoveel als mogelijk kunnen aansluiten op internationale best practices. Dat vereist een Nederlands OAuth 2.0 toepassingsprofiel dat aansluit bij deze internationale best practices.

Daarnaast zal een burger of medewerker van een bedrijf of overheid gebruik kunnen maken van een webportaal van de Omgevingswet ontwikkeld door de overheid. Dit webportaal fungeert als OAuth 2.0-client, en wel een confidential client. Het webportaal maakt gebruik van RESTful API's die door de Omgevingswet beschikbaar worden gesteld, authenticatie op eindgebruikerniveau vereisen.

2.2 Functioneel toepassingsgebied

Als functioneel toepassingsgebied wordt voorgesteld:

Het gebruik van OAuth 2.0 is verplicht voor applicaties waarbij gebruikers (resource owner) toestemming geven (impliciet of expliciet) aan een dienst (van een derde) om namens hem toegang te krijgen tot specifieke gegevens via een RESTful API.

Het gaat dan om een RESTful API waar de resource owner recht tot toegang heeft.

2.3 Organisatorisch werkingsgebied

De expertgroep adviseert om het organisatorisch werkingsgebied van de standaard overeen te laten komen met het werkingsgebied waarop het 'pas toe of leg uit' principe van toepassing is, te weten:

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

3 Toetsing van standaard aan criteria

Om te bepalen of de standaard opgenomen moet worden op de lijst met open standaarden is deze getoetst aan een aantal criteria. Er zijn vier hoofdcriteria:

1. Toegevoegde waarde
2. Open standaardisatieproces
3. Draagvlak
4. Opname bevordert adoptie

Deze criteria staan beschreven in het rapport, *"Toetsingprocedure en criteria voor indieners en experts"* en staan op de website www.forumstandaardisatie.nl/open-standaarden. Het resultaat van de toetsing zal in dit hoofdstuk per criterium beschreven worden. Voor de volledigheid is tevens de definitie van elk criterium opgenomen. Grijs gearceerde vragen zijn op zichzelf niet doorslaggevend voor het beantwoorden van de hoofdvraag, maar dragen wel bij aan het beeld dat nodig is om de hoofdvraag te beantwoorden.

3.1 Toegevoegde waarde

De interoperabiliteitswinst en andere voordelen van adoptie van de standaard wegen overheidsbreed en maatschappelijk op tegen de risico's en nadelen.

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

3.1.1.1 *Is het functioneel toepassingsgebied goed gedefinieerd?*
Ja, zie paragraaf 2.2.

3.1.1.2 *Is het organisatorisch werkingsgebied goed gedefinieerd?*
Ja, zie paragraaf 2.3.

3.1.1.3 *Is de standaard generiek toepasbaar? (en niet alleen bedoeld voor gegevensuitwisseling met één of een beperkt aantal specifieke organisaties) (toelichtende vraag)*
Ja, de standaarden zijn generiek toepasbaar door alle partijen binnen het beschreven organisatorisch werkingsgebied.

3.1.2 Verhoudt de standaard zich goed tot andere standaarden?

3.1.2.1 *Kan de standaard naast of in combinatie met reeds opgenomen standaarden worden toegepast (d.w.z. de standaard conflicteert niet met reeds opgenomen standaarden)?*
Ja, er bestaat met name samenhang met de 'verplichte' standaard SAML op de lijst open standaarden. Hoewel SAML en OAuth 2.0 ook in combinatie met elkaar te zijn gebruiken, kan mogelijk verwarring ontstaan bij de keuze voor een van deze standaarden. Beide standaarden kunnen in een aantal gevallen gebruikt worden. Wel zijn er verschillen in de situaties waar beide standaarden typisch worden toegepast:

- SAML richt zich op federatieve single-signon. Bij het gebruik van OAuth is juist niet nodig dat sprake is van een federatie.

- SAML wordt veelal gebruikt in omgevingen waar XML wordt gebruikt. Waar RESTful API's worden gebruikt, wordt veelal OAuth 2.0 gebruikt.
- SAML is voor authenticatie en autorisatie en OAuth 2.0 voor autorisatie.

Het functioneel toepassingsgebied (wanneer moet OAuth 2.0 gebruikt worden) is daarom zorgvuldig door de experts vastgesteld zodat er geen overlap is. Het functioneel toepassingsgebied van SAML kan dan ook als volgt blijven:
'Federatieve (web)browser-based single-sign-on (SSO) en single-sign-off. Dat wil zeggen dat een gebruiker na eenmalig inloggen via zijn browser toegang krijgt tot verschillende diensten van verschillende partijen.'

OAuth 2.0 maakt verder gebruik van TLS (verplichte standaard op de lijst) en HTTP (aanbevolen standaard op de lijst).

3.1.2.2 *Biedt de aangemelde standaard meerwaarde boven reeds opgenomen standaarden met een overlappend functioneel toepassings- en organisatorisch werkingsgebied? (Dit kan ook om een nieuwe versie van dezelfde standaard gaan.)*
Ja, er zijn geen standaarden met een overlappend functioneel toepassingsgebied gevonden die reeds zijn opgenomen.

3.1.2.3 *Biedt de aangemelde standaard meerwaarde boven bestaande concurrerende standaarden die in aanmerking zouden kunnen komen voor opname? (toelichtende vraag)*
Gedeeltelijk functioneel overlappende standaarden zijn Kerberos (vooral gebruikt op interne netwerken), WS-Federation (enigszins vergelijkbaar met SAML) en FIDO (een standaard voor sterke authenticatie van gebruikers voor onlinediensten).

OpenID Connect bouwt voort op OAuth 2.0 en voegt daaraan de mogelijkheid toe om identiteitsgegevens uit te wisselen.

3.1.2.4 *Is de standaard een internationale standaard of sluit de standaard aan bij relevante internationale standaarden? (toelichtende vraag)*
Ja, OAuth 2.0 (in beheer bij IETF) is een internationale standaard.

3.1.2.5 *Draagt de standaard voldoende bij aan interoperabiliteit zonder dat aanvullende standaardisatieafspraken (zoals lokale profielen) noodzakelijk zijn? (toelichtende vraag)*
Nee, aanvullende keuzes kunnen helpen de interoperabiliteit te verbeteren. OAuth 2.0 is een *framework* dat nog ingevuld en aangepast moet worden door keuzes en met optionele onderdelen.

De expertgroep geeft aan dat bij de procedure voor SAML ten onrechte geen nadere afspraken zijn gemaakt over een toepassingsprofiel. Hierdoor zijn er verschillende implementaties ontstaan wat de interoperabiliteit niet ten goede kwam. Ook voor OAuth is het waarschijnlijk dat zonder verdere standaardisatie verschillende implementaties zullen ontstaan die niet interoperabel zullen zijn.[2] Om dit te voorkomen is het advies om eerst te werken aan de aanvullende standaardisatieafspraken alvorens het gebruik van de standaard verder te verplichten.

2 http://tools.ietf.org/html/rfc6749#section-1.8

3.1.3 *Wegen de kwantitatieve en kwalitatieve voordelen van adoptie van de standaard, voor de (semi-)overheid als geheel en voor de maatschappij, op tegen de nadelen?*

3.1.3.1 *Zijn de kosten van implementatie acceptabel en zijn deze kosten bekend en inzichtelijk?*
Ja, het betreft hier gangbare internettechnologie en door ontwikkelaars wordt het gebruik en het toepassen van de standaard als minder complex ervaren dan de SAML-standaard. Kosten van implementatie kunnen daardoor als acceptabel worden gezien. Overigens is niet bekend wat de exacte kosten voor implementatie zijn.

3.1.3.2 *Is er een (kwalitatieve) business case van de standaard aanwezig? (toelichtende vraag)*
Nee, wel zijn er op internet vergelijkingen te vinden ten aanzien tussen SAML en OAuth 2.0 in combinatie met OpenID Connect, bijvoorbeeld in dit onderzoek van Surf: https://blog.surfnet.nl/wp-content/uploads/2013/04/SURFnet-OpenID-Connect-1.1-.pdf. Ook zijn er beschrijvingen van de voordelen van OAuth 2.0, zoals in https://apigee.com/about/blog/technology/oauth-next-big-thing-security.

3.1.3.3 *Is de meerwaarde van de standaard goed inzichtelijk te maken? Wat betekent de standaard voor de (bedrijfs)processen van een organisatie of keten en wat los je met de standaard op? (toelichtende vraag)*
De meerwaarde van de standaard is dat aanbieders van onlinediensten geen (gevoelige) inloggegevens van gebruikers hoeven te kennen om wel gebruik te maken van andere onlinediensten en -gegevens waar deze gebruiker toegang toe heeft. Daarmee nemen privacyrisico's en risico's op identiteitsdiefstal en misbruik van identiteitsgegevens af. Hierdoor zijn web- en mobiele applicaties op een veilige manier te integreren met elkaar. Veel met name mobiele diensten maken gebruik van RESTful API's om met elkaar te kunnen communiceren. Vaak gaat het daarbij om open niet privacygevoelig informatie. Als dit wel het geval is kan de standaard OAuth 2.0 gebruik worden om de autorisatie te verzorgen.

3.1.3.4 *Zijn de beveiligingsrisico's aan overheidsbrede adoptie van de standaard acceptabel?*
Ja, in principe zorgt de standaard voor extra beveiliging (zie beantwoording voorgaande vraag).

3.1.3.5 *Zijn de privacyrisico's aan overheidsbrede adoptie van de standaard acceptabel?*
Ja, de privacyrisico's nemen juist af (zie beantwoording voorgaande vraag).

3.1.4 *Conclusie criteria 'Toegevoegde waarde'*
Met de standaard is mogelijk dat aanbieders van onlinediensten geen (gevoelige) inloggegevens van gebruikers hoeven te vragen en te bewaren om gebruik te maken van andere onlinediensten en gegevens waar deze gebruiker toegang toe heeft. Daarmee nemen privacyrisico's en risico's op identiteitsdiefstal en misbruik van identiteitsgegevens af.

Er bestaat met name samenhang met de 'verplichte' standaard SAML op de lijst open standaarden. Hoewel SAML en OAuth 2.0 ook in combinatie met elkaar te zijn gebruiken, kan mogelijk verwarring ontstaan bij de keuze voor een van deze standaarden. Ook kunnen in een aantal gevallen

beide standaarden gebruikt worden. Het functioneel toepassingsgebied (wanneer moet OAuth 2.0 gebruikt worden) is daarom zorgvuldig door de experts vastgesteld zodat er geen overlap is.

Wel dient nog een toepassingsprofiel te worden vastgesteld, waarmee de interoperabiliteit binnen de overheid (en eventueel daarbuiten) geborgd wordt.

3.2 Open standaardisatieproces

De ontwikkeling en het beheer van de standaard zijn op een open, onafhankelijke, toegankelijke, inzichtelijke, zorgvuldige en duurzame wijze ingericht.

3.2.1 Is de documentatie voor een ieder drempelvrij beschikbaar?

3.2.1.1 *Is het specificatiedocument beschikbaar zonder dat er sprake is van onacceptabele belemmeringen (zoals te hoge kosten en te hoge lidmaatschapseisen)?*
Ja, voor OAuth 2.0 zijn de specificaties beschikbaar op https://datatracker.ietf.org/wg/oauth/documents. Het gaat dan om:

RFC6749	The OAuth 2.0 Authorization Framework
RFC6750	The OAuth 2.0 Authorization Framework: Bearer Token Usage
RFC6755	An IETF URN Sub-Namespace for OAuth
RFC6819	OAuth 2.0 Threat Model and Security Considerations
RFC7009	OAuth 2.0 Token Revocation
RFC7519	JSON Web Token (JWT)
RFC7521	Assertion Framework for OAuth 2.0 Client Authentication and Authorization Grants
RFC7522	Security Assertion Markup Language (SAML) 2.0 Profile for OAuth 2.0 Client Authentication and Authorization Grants
RFC7523	JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants
RFC7591	OAuth 2.0 Dynamic Client Registration Protocol
RFC7592	OAuth 2.0 Dynamic Client Registration Management Protocol
RFC7636	Proof Key for Code Exchange by OAuth Public Clients
RFC7662	OAuth 2.0 Token Introspection
RFC7800	Proof-of-Possession Key Semantics for JSON Web Tokens (JWTs)

3.2.1.2 *Is de documentatie over het ontwikkel- en beheerproces (bijv. het voorlopige specificatiedocument, notulen en beschrijving besluitvormingsprocedure) beschikbaar zonder dat er sprake is van onacceptabele belemmeringen (zoals te hoge kosten en te hoge lidmaatschapseisen)?*
Ja, OAuth 2.0 wordt beheerd door IETF dat bekend staat als een open beheerorganisatie. IETF beheert ook enkele andere standaarden die reeds op de lijst open standaarden staan. OAuth 2.0 wordt IETF op dezelfde wijze beheerd als deze andere standaarden.

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

3.2.2.1 *Stelt de standaardisatieorganisatie het intellectueel eigendomsrecht op de standaard m.b.t. bijvoorbeeld eventuele patenten- onherroepelijk royalty-free voor eenieder beschikbaar?*

Ja, voor OAuth 2.0 is dit door IETF geregeld in https://www.ietf.org/rfc/rfc3979.txt.

3.2.2.2 *Garandeert de standaardisatieorganisatie dat partijen die bijdragen aan de ontwikkeling van de standaard hun intellectueel eigendomsrecht onherroepelijk royalty-free voor eenieder beschikbaar stellen?*
Ja, voor OAuth 2.0 is dit door IETF geregeld in https://www.ietf.org/rfc/rfc3979.txt.

3.2.3 Is de inspraak van eenieder in voldoende mate geborgd?

3.2.3.1 *Is het besluitvormingsproces toegankelijk voor alle belanghebbenden (bijv. gebruikers, leveranciers, adviseurs, wetenschappers)?*
Ja, voor IETF is dit toegankelijk.

3.2.3.2 *Vindt besluitvorming plaats op een wijze die zoveel mogelijk recht doet aan de verschillende belangen?*
Ja, voor IETF is de besluitvorming toegankelijk.

3.2.3.3 *Kan een belanghebbende formeel bezwaar aantekenen tegen de gevolgde procedure?*
Onbekend, daarvoor kan geen aanwijzing gevonden worden bij IETF.

3.2.3.4 *Organiseert de standaardisatieorganisatie regelmatig overleggen met belanghebbenden over doorontwikkeling en beheer van de standaard? (toelichtende vraag)*
Ja, IETF organiseert regelmatig activiteiten rondom de beheerde standaarden.

3.2.3.5 *Organiseert de standaardisatieorganisatie een publieke consultatie voordat (een nieuwe versie van) de standaard wordt vastgesteld? (toelichtende vraag)*
Ja, voor IETF is dit toegankelijk.

3.2.4 Is de standaardisatieorganisatie onafhankelijk en duurzaam?

3.2.4.1 *Is de ontwikkeling en het beheer van de standaard belegd bij een onafhankelijke non-profit standaardisatieorganisatie?*
Ja, IETF is een non-profitorganisatie.

3.2.4.2 *Is de financiering van de ontwikkeling en het onderhoud van de standaard voor tenminste drie jaar gegarandeerd?*
Ja, ondanks dat dit niet formeel is vastgelegd, is de verwachting (gezien de internationale organisaties die OAuth 2.0 ondersteunen en de wereldwijde adoptie) dat de financiering de komende drie jaar gegarandeerd is.

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

3.2.5.1 *Heeft de standaardisatieorganisatie gepubliceerd beleid met betrekking tot versiebeheer van de standaard? (met o.a. aandacht voor migratie van gebruikers) (toelichtende vraag)*
Ja, bij IETF zijn oude versies terug te vinden. Ook zijn er werkgroepen bezig met versiebeheer.

3.2.5.2 *Is de beheerdocumentatie goed vindbaar en verkrijgbaar? (toelichtende*

vraag)
Ja, zie voor OAuth 2.0: https://datatracker.ietf.org/wg/oauth/documents/.

3.2.5.3 *Is het belang van de Nederlandse overheid voldoende geborgd bij de ontwikkeling en het beheer van de standaard? (toelichtende vraag)*
De standaard wordt beheerd door een internationale standaardisatieorganisatie. Het belang van de Nederlandse overheid is niet specifiek geborgd. De expertgroep ziet hier geen belemmeringen in.

3.2.5.4 *Is de vertegenwoordiging van belanghebbenden bij het beheer van de standaard een goede representatie van het werkingsgebied en functioneel toepassingsgebied van de standaard? (toelichtende vraag)*
De standaard wordt beheerd door een internationale standaardisatieorganisatie. Partijen uit het werkingsgebied zijn niet zelf specifiek vertegenwoordigd. De expertgroep ziet hier geen belemmeringen in.

3.2.5.5 *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? (toelichtende vraag)*
Nee, het standaardisatieproces op zich is goed geregeld, maar doordat niet specifiek het Nederlandse belang is vertegenwoordigd is het altijd goed om de impact van nieuwe versies te onderzoeken.

3.2.6 Is er adoptieondersteuning voor de standaard?

3.2.6.1 *Is er een toegankelijk aanspreekpunt of organisatie waar meer informatie over de standaard is te vinden en valt op te vragen?*
Er is geen aparte community voor de standaard, maar genoeg developers communities met fora waar informatie over gebruik en toepassing van de standaard is te vinden. Er is veel informatie op internet beschikbaar. Verder zijn er verschillende partijen actief in de Nederlandse markt die ondersteuning bieden.

3.2.6.2 *Wordt er ondersteuning gegeven in de adoptie en de implementatie van de standaard?*
Voor OAuth 2.0 is er geen centraal aanspreekpunt voor adoptie en implementatie. Wel heeft Surf verschillende blogs geschreven over de implementatie van de standaard en een bijeenkomst over de standaard georganiseerd. https://blog.surf.nl/instellingsdiensten-toegankelijk-via-mobiele-interfaces-een-afweging-tussen-gebruiksvriendelijkheid-en-beveiliging/.

3.2.7 Conclusie criteria 'Open standaardisatieproces'
De expertgroep concludeert dat het standaardisatieproces van IETF voldoende open is. OAuth 2.0 is een internationale standaard waarbij de Nederlandse overheid haar belang niet direct heeft geborgd. De experts zijn van mening dat dat vanwege het feit dat het hier om een internationale standaard gaat ook niet noodzakelijk is. Ondanks deze (geringe) beperkingen concludeert de expertgroep dat het standaardisatieproces van IETF voldoende open is.

Het standaardisatieproces voldoet aan alle hoofdcriteria (maar niet aan enkele grijs-gearceerde criteria). Het beheer van de standaard voldoet daardoor niet aan de criteria voor 'uitstekend beheerproces'.

3.3 Draagvlak

Aanbieders en gebruikers moeten voldoende ervaring hebben bij het ondersteunen, implementeren en gebruiken van de standaard.

3.3.1 Bestaat er voldoende marktondersteuning voor de standaard?

3.3.1.1 *Bieden meerdere leveranciers ondersteuning voor de standaard?*

3.3.1.2 *Kan een gebruiker de conformiteit van de implementatie van de standaard (laten) toetsen? (toelichtende vraag)*
Ja, er zijn meerdere leveranciers die diensten bieden bij implementatie van de standaard OAuth 2.0.

3.3.1.3 *Draagt de standaard voldoende bij aan interoperabiliteit zonder dat aanvullende standaardisatieafspraken (zoals lokale profielen) noodzakelijk zijn om de standaard te implementeren of te gebruiken?*
Voor OAuth 2.0 moeten aanvullende afspraken in de vorm van een overheidstoepassingsprofiel gemaakt worden. Zonder vastgesteld toepassingsprofiel is de interoperabiliteit binnen de overheid (en eventueel daarbuiten) niet geborgd. Iedereen zal dan zijn eigen implementantie verzorgen, wat de beoogde interoperabiliteit niet ten goede komt. Onderdeel van het toepassingsprofiel zou onder andere moeten zijn: welke flows ondersteund worden, afspraken over het accesstoken, toepassing van security considerations en afspraken over de eventuele doorgifte van identiteitsgegevens.

3.3.1.4 *Zijn er referentieprofielen of voorbeeldimplementaties van de standaard aanwezig en zijn deze referentieprofielen vrij te gebruiken? (toelichtende vraag)*
OpenID Connect en User-Managed Access (UMA) zijn profielen die gebruikt zouden kunnen worden. OpenID Connect geeft een mogelijke invulling van OAuth 2.0, specifiek gericht op uitwisseling van identiteitsgegevens. UMA voorziet in een specifiek gebruikersscenario waarin de gebruik zelf beheert welke applicaties welke toegangsrechten hebben. Beide zijn daardoor niet algemeen genoeg om te dienen als overheidstoepassingsprofiel. De experts geven er daarom de voorkeur aan om een overheidstoepassingsprofiel op te stellen voor OAuth 2.0.

3.3.2 Kan de standaard rekenen op voldoende draagvlak?

3.3.2.1 *Staan de belangrijkste stakeholders vanuit de overheid voor deze standaard achter de adoptie van de standaard?*
Vanuit verschillende overheidsorganisaties is interesse getoond om de standaard te toetsen (Rijkswaterstaat/ Logius (DigiD) / Belastingdienst). Ook was er veel animo voor de expertbijeenkomst, zowel de eerste als de tweede keer. Dit toont ook wel de interesse en de vraag naar het onderwerp aan.

3.3.2.2 *Staan de overheidsorganisaties die daadwerkelijk worden geraakt door een mogelijke verplichting van de standaard achter het gebruik van de standaard?*
Ja, met de verplichting indachtig hebben de experts, waaronder van de betrokken overheidsorganisaties, het functioneel toepassingsgebied

nauwkeurig afgebakend. De volgende organisaties zouden met name geraakt kunnen worden:
- aanbieders van authenticatie- en autorisatiediensten, zoals DigiD, eHerkenning en Idensys, en
- aanbieders van onlinediensten waarvoor ingelogd moet worden, zoals vergunningaanvragen op websites van overheden.

3.3.2.3 *Wordt de aangemelde versie van de standaard binnen het organisatorische werkingsgebied door meerdere organisaties gebruikt?*
In ieder geval wordt binnen het hoger onderwijs gebruik gemaakt van OAuth 2.0 als standaard (bijvoorbeeld Surf en UvA). Daarnaast heeft de Omgevingswet/Laan van de Leefomgeving de standaard opgenomen in hun doelarchitectuur.

3.3.2.4 *Wordt een vorige versie van de standaard binnen het organisatorische werkingsgebied door meerdere organisaties gebruikt? (toelichtende vraag)*
Niet bekend.

3.3.2.5 *Is de aangemelde versie backwards compatible met eerdere versies van de standaard? (toelichtende vraag)*
Nee, OAuth 2.0 is niet backwards compatible met OAuth 1.

3.3.2.6 *Zijn er voldoende positieve signalen over toekomstige gebruik van de standaard door (semi-)overheidsorganisaties, het bedrijfsleven en burgers? (toelichtende vraag)*
Experts van de betreffende overheidsorganisaties geven aan interesse te hebben. Naast het domein van de Omgevingswet is er ook binnen de governance van het 'afsprakenstelsel elektronische toegangsdiensten' (ook bekend als eHerkenning/Idensys) een voorstel uitgewerkt om OAuth 2.0 te gebruiken voor authenticatie ten behoeve van diensten vanuit "native apps". Dit voorstel ligt ter besluitvorming voor.

In het bedrijfsleven wordt de standaard reeds volop gebruikt, zoals bij LinkedIn, Facebook, Apple, Google, Amazon AWS en Microsoft Azure.

3.3.3 *Conclusie criteria 'Draagvlak'*
De expertgroep concludeert dat het draagvlak voor OAuth 2.0 voldoende is. Hoewel de standaard nog niet door veel overheidsorganisaties wordt gebruikt, zijn er voldoende signalen dat dit in de toekomst zal toenemen. Toekomstige gebruikers kunnen hierbij rekenen op voldoende ondersteuning, in de vorm van expertise bij marktpartijen en implementaties in software, voor de implementatie en bij het gebruik van de standaard.

3.4 Opname bevordert adoptie

De opname op de lijst is een geschikt middel om de adoptie van de standaard te bevorderen.

Er zijn twee lijsten: de lijst met aanbevolen (gangbare) standaarden en de lijst voor 'pas toe of leg uit'. Deze laatste lijst is bedoeld om standaarden een extra stimulans te geven wanneer:
1. Hun huidige adoptie binnen de (semi-)overheid beperkt is;
2. Opname bijdraagt aan de adoptie door te stimuleren o.b.v. het 'pas toe of leg uit'-regime.

De lijst met aanbevolen (gangbare) standaarden vormt een referentie voor standaarden die veel gebruikt worden. Als standaarden voldoen aan enkele basisvoorwaarden (voor o.a. openheid), er is geen discussie over en de standaarden worden breed gebruikt, dan vindt opname op die lijst plaats.

Het Forum Standaardisatie heeft geconcludeerd dat het voor de aanbevolen standaarden op de lijst ook verstandig is om standaarden mee te nemen die nog eerder in de levensfase zitten: standaarden die wel zijn vastgesteld maar nog niet regulier/breed gebruikt worden en veelbelovend zijn in toepassing in de nabije toekomst dan wel een bestaande standaard (op de lijst) vervangen en standaarden die in de nabije toekomst naar verwachting gangbaar worden.

3.4.1 *Is de "pas toe of leg uit" het passende middel om de adoptie van de standaard binnen de (semi)overheid te bevorderen?*
Ja, plaatsing op de lijst open standaarden met de status 'pas toe of leg uit' biedt overheden houvast en een duidelijk signaal dat OAuth 2.0 de te verkiezen standaard is. Het gebruik van OAuth 2.0 is groeiend met name ook daar waar een gebruiker webapplicaties en mobiele applicaties toegang geeft tot zijn andere diensten en gegevens waar de gebruiker toe gerechtigd is. Voor implementatie zijn er slechts enkele concrete plannen bekend. De adoptie van de standaard heeft daarom een extra stimulans nodig. Wel is het daarbij belangrijk om een gemeenschappelijk toepassingsprofiel te ontwikkelen zodat voorkomen wordt dat er verschillende implementaties ontstaan.

3.4.2 *Is de status aanbevolen het passende middel om de adoptie van de standaard binnen de (semi)overheid te bevorderen?*
Nee, het gebruik van OAuth 2.0 heeft nog niet de omvang die nodig is om de standaard als gangbaar te kunnen beschouwen.

3.4.3 *Conclusie criteria 'Opname bevordert adoptie'*
De expertgroep concludeert dat de 'pas toe of leg uit'-lijst het passende middel is om de adoptie van de standaard binnen de (semi)overheid te bevorderen.

4 Adoptieactiviteiten

Gebruik van de standaard is het einddoel van het Forum en College. Plaatsing op de lijsten is hiervoor een goede stap, maar voor het daadwerkelijk adopteren (implementeren en gebruiken) van de standaard is vaak aanvullende actie benodigd. Aanvullend kan Forum Standaardisatie dan ook bijdragen aan adoptie van de standaard door het actief inzetten van adoptie-instrumenten of ondersteunende acties. Welke kansen zijn er om de adoptie te versnellen en welke drempels bestaan er die de adoptie van de standaard hinderen?

In dit deel wordt in kaart gebracht welke kansen er zijn om de adoptie te versnellen en welke drempels er bestaan die de adoptie van de standaard hinderen. Aanvullend kan Forum Standaardisatie bijdragen aan adoptie van de standaard door het actief inzetten van adoptie-instrumenten of ondersteunende acties. Tot slot beantwoordt dit deel de vragen of en op welke termijn de adoptievoorgang van de standaard het best nog eens geëvalueerd kan worden.

De expertgroep doet het Forum standaardisatie de aanbeveling om de volgende stappen te zetten en te streven naar opname van de standaard op de lijst voor 'pas toe of leg uit':

1. Aanbevolen wordt om de experts van deze experttoets tezamen met Logius (als beheerder van DigiD, eHerkenning en Idensys), het Ministerie van EZ (ivm. buitenlandse relaties in het kader van de eIDAS-verordening) en RvIG een toepassingsprofiel te laten opstellen voor de toepassing van OAuth 2.0, om variaties in de implementatie te voorkomen. De experts hebben daartoe reeds een aantal te hanteren uitgangspunten in de expertbijeenkomst met elkaar afgestemd:
   - Alleen de implicit flow en autorisatiecode flow worden toegepast (de client credentials flow wordt niet toegepast)
   - Een baseline voor een accesstoken is nog op te stellen (opslag, gebruik van secure SSL, geldigheid, etc.)
   - De security considerations van OAuth 2.0 dienen verplicht toegepast te worden (incl. de toevoegingen van IETF OAuth WG), maar alleen waar dat nodig is voor interoperabiliteit
   - Het doorgeven van vastgestelde identiteiten dient door de overheid met een voldoende krachtig token te gebeuren en op eenduidige wijze (het formaat en de claims binnen overheid eenduidig vastleggen)
   - De semantische standaardisatie van identiteitsgegevens is nog vast te leggen.

   Om te komen tot het gemeenschappelijk toepassingsprofiel zou het Forum Standaardisatie hierbij in eerste instantie de rol van secretariaat op zich moeten nemen.

2. Vervolgens wordt aanbevolen 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.