Forum Standaardisatie
www.forumstandaardisatie.nl
forumstandaardisatie@logius.nl
Bureau Forum Standaardisatie
gehuisvest bij Logius
Postadres
Postbus 96810
2509 JE Den Haag
Bezoekadres
Wilhelmina van Pruisenweg 52
2595 AN Den Haag
Bij bezoek aan Logius is legitimatie verplicht

notitie

Opname OAuth 2.0-standaard op de lijst met open standaarden

FORUM STANDAARDISATIE

Agendapunt:	FS 170419.2B
Betreft:	Opname OAuth 2.0-standaard op de lijst met open standaarden
Aan:	Forum Standaardisatie
Van:	Stuurgroep Standaardisatie
Datum:	6 april 2017

Aanleiding en achtergrond

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. 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, maar voor implementatie zijn er slechts enkele concrete plannen bekend. De adoptie van de standaard heeft daarom een extra stimulans nodig.

Betrokkenen en 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] Op basis van dit besluit is de expertgroep op 7 juli 2016 en 22 september 2016 bijeengekomen om de standaard, de aandachtspunten en openstaande vragen uit het voorbereidingsdossier te bespreken. Tijdens deze bijeenkomst is ook het advies ten aanzien van het functioneel toepassingsgebied vastgesteld. Het expertadvies is beschikbaar gesteld voor publieke consultatie. Dit heeft drie reacties opgeleverd.

[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).*

Consequenties en vervolgstappen

De expertgroep vindt het belangrijk om een gemeenschappelijk toepassingsprofiel te ontwikkelen zodat voorkomen wordt dat er verschillende implementaties ontstaan. Het advies is om in eerste instantie te starten met een basisprofiel met een algemeen karakter en algemene uitgangspunten. Omdat als zo'n profiel diep uitgewerkt moet worden met dito beheer dan is het risico dat niemand daarvoor de verantwoordelijkheid neemt.

Gevraagd besluit

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

Het Forum Standaardisatie adviseert het Nationaal Beraad Digitale Overheid om:
1. voor de overheid basis toepassingsprofiel voor OAuth 2.0 te ontwikkelen, en
2. de opname van OAuth 2.0 op de lijst voor 'pas toe of leg uit' aan te houden tot dit toepassingsprofiel voor OAuth 2.0 is opgesteld.

Ad 1
Aanbevolen wordt om de experts van de experttoets een toepassingsprofiel te laten opstellen voor de toepassing van OAuth 2.0, om variaties in de implementatie te voorkomen. De experts zijn vertegenwoordigers van marktpartijen en overheidsorganisaties, zoals Logius, RDW, SURFnet, Kennisnet, Kadaster, Geonovum, RvIG, DICTU en de RVO. Aanbevolen wordt een toepassingsprofiel te laten opstellen door deze experts tezamen met Logius (als beheerder van DigiD, eHerkenning en Idensys), het Ministerie van EZ (ivm. buitenlandse relaties in het kader van de eIDAS-verordening). 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 voor de overheid zou het Forum Standaardisatie hierbij in eerste instantie de rol van secretariaat op zich moeten nemen. Later zou deze rol door iemand anders overgenomen moeten worden als blijkt dat het nodig is dat het profiel actief beheer moet worden.

Ad 2
Als functioneel toepassingsgebied voor OAuth 2.0 wordt geadviseerd:

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 van OAuth 2.0 wordt geadviseerd:

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

Toelichting

1. 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.

2. Hoe is het proces verlopen?
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.[2]

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. Het expertadvies vat de uitkomsten van de discussie en toetsing samen.

Het expertadvies is van 24 februari tot 25 maart 2017 beschikbaar gesteld voor publieke consultatie. Dit heeft drie reacties opgeleverd. Na verwerking van deze reacties is dit forumadvies opgesteld.

[2] *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).*

3. Hoe scoort de standaard op de toetsingscriteria?

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'.

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.

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
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. Het gebruik van OAuth 2.0 heeft nog niet de omvang die nodig is om de standaard als gangbaar te kunnen beschouwen. 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 waardoor er nog steeds geen sprake is van interoperabiliteit.

Toelichting van eventuele risico's
De standaard zorgt juist voor extra beveiliging en de privacyrisico's nemen daardoor af. 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.

4. Wat is de conclusie van de expertgroep en de consultatie?

Conclusie van de expertgroep
Aan het Nationaal Beraad wordt geadviseerd om OAuth 2.0 op te nemen op de lijst met open standaarden met de status 'pas toe of leg uit'.

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 voorgesteld:

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

Eventuele aanvullingen vanuit de consultatie
Op de openbare consultatie van het expertadvies zijn drie reacties ontvangen (van Belastingdienst, Logius en het Centraal Informatiebeveiligingsoverleg van de provincies (CIBO)). De reacties zijn positief, onderschrijven het belang van de standaard en opname op de 'pas toe of leg uit'-lijst en onderschrijven het belang van de voorwaarde om eerst een gemeenschappelijk toepassingsprofiel op te stellen. Zij stellen echter ook de volgende nadere aspecten ter discussie.

Logius
Kort gezegd heeft Logius opmerkingen gemaakt over:
- Opstellen gemeenschappelijk toepassingsprofiel dient rekening te houden met andere ontwikkelingen in het authenticatie- en autorisatielandschap
  Reactie: voor het opstellen zal ook vertegenwoordiging uit het eID-programma en andere programma's worden gevraagd.
- Er zal een beheerorganisatie moeten komen voor gemeenschappelijk toepassingsprofiel
  Reactie: dit zal worden meegenomen bij het opstellen van het gemeenschappelijk toepassingsprofiel, maar is mogelijk wel een grote belemmering voor het in eerste instantie opnemen op de lijst.

CIBO
Het CIBO heeft opmerkingen gemaakt over:

- Randvoorwaarden te stellen aan OAuth 2.0 providers en de vraag of een Rijks OAuth 2.0 provider zal worden ingericht
  Reactie: vooralsnog is er geen plan voor een Rijks OAuth 2.0 provider. Bij het opstellen van het gemeenschappelijk toepassingsprofiel zullen ook de daarbij bijbehorende randvoorwaarden aan providers worden meegenomen.
- Vertegenwoordiging bij het opstellen van het gemeenschappelijk toepassingsprofiel
  Reactie: gemeenten en provincies en hun overleggen op het gebied van security en privacy zullen worden uitgenodigd om deel te nemen aan het overleg voor het opstellen van een gemeenschappelijk toepassingsprofiel.

Belastingdienst
De Belastingdienst onderschreef het expertadvies en had geen verder inhoudelijk commentaar.

5. Welke additionele adviezen zijn er ten aanzien van de adoptie van de standaard?
Naar aanleiding van de expertgroep zijn er bij opname op de lijst met open standaarden de volgende oproepen ten aanzien van de adoptie van de standaard te doen:

1. vóór plaatsing op de lijst is het opstellen van een gemeenschappelijk toepassingsprofiel voor de overheid van belang.

De opgeroepen partijen worden gevraagd om één jaar na opname van de standaard over de voortgang op deze punten te rapporteren aan het Forum Standaardisatie.

Bijlage

- Expertadvies OAuth 2.0.
- Overzicht reacties consultatieronde