Forum Standaardisatie

Wilhelmina van Pruisenweg 52
2595 AN Den Haag

Postbus 96810
2509 JE Den Haag

www.forumstandaardisatie.nl

notitie

Aan:	Forum Standaardisatie		
Van:	Bureau Forum Standaardisatie		
Datum:	28 maart 2017	**Versie**	1.0
Betreft:	Overzicht reacties openbare consultatieronde OAuth 2.0		
Bijlagen:	1. Reactie CIBO 2. Reactie Logius 3. Reactie Belastingdienst		

1. Reactie CIBO

Van: Wekema M.
Datum: 24 maart 2017 12:50:35 CET
Aan: 'Anneke Spijker'
Onderwerp: Antw.: Aanmelden van standaarden en Reminder openbare consultatie

Hallo Anneke,
Hierbij de review van de standaarden.
Deze zijn afgelopen dinsdag in het CIBO besproken en goedgekeurd.
Kun jij zorgen dat deze worden aangeleverd?

Met vriendelijke groet,
Michel Wekema
Voorzitter CIBO

Vragen over het Forumadvies
("Forumadvies en Managementsamenvatting")

Vraag:
1. Bent u het eens met het advies van de expertgroep om Oauth2.0 met een 'pas toe of leg uit'-verplichting op te nemen op de lijst met open standaarden nadat er een gemeenschappelijk toepassingsprofiel is ontwikkeld?

Antwoord: ten dele. Er wordt niet in gegaan op de benodigde randvoorwaarden die er aan een OAuth 2.0 provider gesteld moet worden. Is het de bedoeling dat elke "provider" geaccepteerd wordt? Of komt er een Rijks OAuth 2.0 provider?

Vragen over hoofdstuk 1 van het expertadvies
("Doelstelling expertadvies")
Hoofdstuk 1 geeft een beschrijvende toelichting over de doelstelling van het expertadvies.

Vraag:
2. Zijn er volgens u in deze aanvullingen of anderszins wijzigingen nodig in paragrafen 1.5, 'samenstelling expertgroep' (bezien vanuit het doel van de procedure om zoveel mogelijk belanghebbende te betrekken)?

Antwoord: Ja uitbreiding is zeker nodig. Denk aan gemeenten en andere instanties waarbij veelvuldig e-loket functionaliteit gebruikt worden.

Vragen over hoofdstuk 2 van het expertadvies
("Toepassings- en werkingsgebied")

Hoofdstuk 2 geeft een toelichting op de standaarden en gaat achtereenvolgens in op het voorgestelde functionele toepassingsgebied en het voorgestelde organisatorische werkingsgebied.

Vragen:

3. Bent u het eens met het door de expertgroep geadviseerde functionele toepassingsgebied? [paragraaf 2.1 van het expertadvies]?

Antwoord: Ja, mits duidelijk de eerder gestelde randvoorwaarde bij vraag 1 gehonoreerd wordt.

4. Bent u het eens met het door de expertgroep geadviseerde organisatorische werkingsgebied? [paragraaf 2.2 van het expertadvies]?

Antwoord: Ja, mits aan de eerder gestelde randvoorwaarde voldaan is.

Vragen over hoofdstuk 3 van het expertadvies
("Toetsing van de standaard aan de criteria")

Hoofdstuk 3 gaat in op de toetsingscriteria (Toegevoegde waarde, Open standaardisatieproces, Draagvlak, Opname bevordert adoptie) en bijbehorende deelaspecten.

Vragen:

5. Bent u het eens met de constateringen en conclusies van de expertgroep inzake de toegevoegde waarde? [paragraaf 3.1 van het expertadvies]?

Antwoord: Ja, mits aan de eerder gestelde randvoorwaarde is voldaan.

6. Bent u het eens met de constateringen en conclusies van de expertgroep inzake het open standaardisatieproces? [paragraaf 3.2 van het expertadvies]?

Antwoord: Deels, het verplichten van de OAuth betekent ook dat de overheid hier een actieve rol heeft, meer dan alleen toepassen. Er zal ook mogelijk een Rijks oAuth 2.0 provider opgezet moeten worden.

7. Bent u het eens met de constateringen en conclusies van de expertgroep inzake het draagvlak? [paragraaf 3.3 van het expertadvies]?

Antwoord: er moet heel goed beschreven worden wanneer welke standaard gebruikt dient te worden. SAML leent zich heel erg goed voor bedrijven en organisaties, terwijl OAuth 2.0 meer voor individuen geschikt zal zijn. Maak daarom onderscheidt tussen “bugers” en bedrijven/organisaties voor het verplicht stellen van de beoogde standaard.

8. Bent u het eens met de constateringen en conclusies van de expertgroep inzake de bevordering van de adoptie door opname op de lijst? [paragraaf 3.4 van het expertadvies]?

Antwoord: bij 3.1.2.1 staat HTTP als afhankelijke standaard genoemd. Dit is deels correct, maar er wordt natuurlijk HTTPS vereist, want anders kan TLS niet worden afgedwongen.

Vragen over hoofdstuk 4 van het expertadvies
(“Adoptieactiviteiten")

Vraag:

9. Bent u het eens met de adoptie-aanbevelingen van de expertgroep aan het Nationaal Beraad Digitale Overheid? [hoofdstuk 4 van het expertadvies]

Antwoord: Het punt van " het doorgeven van vastgestelde identiteiten…" kan met SAML al afgevangen worden. Het moet daarom heel duidelijk zijn waarvoor de technieken gebruikt moeten gaan worden. Om OAuth passend te maken voor iets wat SAML al biedt, is de omgekeerde wereld.

Daarnaast heeft de " gebruiker" bij OAuth meer mogelijkheden om een reeds verstrekt token "invalid" te maken, iets wat SAML weer niet heeft. Des te meer reden om eerst na te denken over wat we als overheid nu precies hiermee willen gaan doen. Kortom het is terecht om eerst over een toepassingsprofiel na te denken.
Resterende inhoudelijke opmerkingen

Vraag:

10. Is/zijn er volgens u nog andere informatie of overwegingen die aan het Forum en Nationaal Beraad Digitale Overheid zou moeten worden meegegeven voor een besluit over het opnemen van deze standaard op de 'pas toe of leg uit'-lijst?

Antwoord: wees je bewust van de mogelijkheden en onmogelijkheden i.c.m. het nog op te stellen toepassingsprofiel. Hou daarbij rekening met alle type overheidsorganisaties en de eerder genoemde randvoorwaarden.

2. Reactie Logius

Van: Leijnse, P (Peter) – Logius
Verzonden: vrijdag 24 maart 2017 15:22
Aan: Forum standaardisatie
Onderwerp: Consultatie HTTPS/HSTS en OAuth 2.0

Beste collega,

Bijgaand de reactie vanuit Logius op de consultaties van HTTPS/HSTS en OAuth 2.0. Bij vragen altijd bereid tot toelichting.

Met vriendelijke groet,
Peter Leijnse
Lead architect I&S

Vragen over het Forumadvies
("Forumadvies en Managementsamenvatting")

Vraag:
11. Bent u het eens met het advies van de expertgroep om Oauth2.0 met een 'pas toe of leg uit'-verplichting op te nemen op de lijst met open standaarden nadat er een gemeenschappelijk toepassingsprofiel is ontwikkeld?

Het ontwikkelen van een specifiek profiel op OAuth 2.0 zonder daarbij rekening te houden met andere ontwikkelingen in het authenticatie- en autorisatielandschap achten wij voorbarig. Of een gemeenschappelijk toepassingsprofiel kan worden ontwikkeld en hoe, hangt samen met het antwoord op twee vragen:

1. Hoe verhoudt het gebruik van Oauth 2.0 zich met de ontwikkeling van het stelsel van elektronische toegangsdiensten?
2. Op welke wijze wil de Nederlandse overheid betrouwbaar en veilig gegevens uitwisselen met gebruikmaking van de REST-stijl?

Momenteel wordt ingezet op het ontwikkelen van een samenhangend federatief toegangsstelsel (eID, ETD) dat door de voorgenomen wet GDI een verplichtend karakter zal krijgen voor alle bestuursorganen. Binnen dit stelsel is vooralsnog gekozen voor het gebruik van SAML. Een toepassingsprofiel van OAuth 2.0 naast de reeds afgesproken standaarden is voorstelbaar en relevant, maar dient niet buiten de reeds ingezette ontwikkelingen te worden geplaatst. Alleen dan kan worden voorkomen dat overheidspartijen worden geconfronteerd met onsamenhangende of tegenstrijdige eisen.

De argumentatie in het advies stoelt op een sterke samenhang tussen REST en OAuth. Een te ontwikkelen toepassingsprofiel zou zich moeten richten op de interoperabiliteit van overheidsservices die op basis van REST-principes worden aangeboden. Partijen die diensten ontwikkelen die met dergelijke overheidsservices communiceren zijn gebaat bij een toepassingsprofiel dat alle aspecten van de inzet van REST afdekt, niet

alleen de authenticatie. Vergelijk bijvoorbeeld met de Digikoppeling-standaard, waar communicatie, beveiliging en techniek voor een aantal standaarden samenhangend zijn geregeld. Een vergelijkbare standaard daarnaast (of een extra profiel naast ebMS en WUS) zou een waardevolle toevoeging zijn.
NB: interactie op basis van REST en op basis van (huidige) Digikoppeling kunnen ons inziens prima naast elkaar bestaan.

Vragen over hoofdstuk 1 van het expertadvies
("Doelstelling expertadvies")

Hoofdstuk 1 geeft een beschrijvende toelichting over de doelstelling van het expertadvies.

Vraag:
12. Zijn er volgens u in deze aanvullingen of anderszins wijzigingen nodig in paragrafen 1.5, 'samenstelling expertgroep' (bezien vanuit het doel van de procedure om zoveel mogelijk belanghebbende te betrekken)?

In ieder geval mist vertegenwoordiging uit het eID-programma, zowel beleidsmatig als inhoudelijk.

Vragen over hoofdstuk 2 van het expertadvies
("Toepassings- en werkingsgebied")

Hoofdstuk 2 geeft een toelichting op de standaarden en gaat achtereenvolgens in op het voorgestelde functionele toepassingsgebied en het voorgestelde organisatorische werkingsgebied.

Vragen:
13. Bent u het eens met het door de expertgroep geadviseerde functionele toepassingsgebied? [paragraaf 2.1 van het expertadvies]?

Het toepassingsgebied is behoorlijk technisch-cryptisch geformuleerd. Het lijkt erop dat het beoogde standaardisatiegebied is 'RESTful-APIs met inzet van OAuth'.

14. Bent u het eens met het door de expertgroep geadviseerde organisatorische werkingsgebied? [paragraaf 2.2 van het expertadvies]?

In hetzelfde organisatorische werkingsgebied worden dezelfde organisaties via Wet GDI waarschijnlijk verplicht om aan te sluiten op authenticatiediensten die op basis van SAML werken.

Vragen over hoofdstuk 3 van het expertadvies
("Toetsing van de standaard aan de criteria")

Hoofdstuk 3 gaat in op de toetsingscriteria (Toegevoegde waarde, Open standaardisatieproces, Draagvlak, Opname bevordert adoptie) en bijbehorende deelaspecten.

Vragen:
15. Bent u het eens met de constateringen en conclusies van de expertgroep inzake de toegevoegde waarde? [paragraaf 3.1 van het expertadvies]?

Er is zeker toegevoegde waarde in het ontwikkelen van een toepassingsprofiel voor RESTful APIs, maar daarbij zijn wel een aantal kanttekeningen te plaatsen.
Het is weliswaar zo dat technisch de toepassing van SAML en OAuth naast elkaar goed af te bakenen zijn op een koppelvlak, maar dat wil nog niet zeggen dat er geen implementatieuitdagingen zijn. Een authenticatiedienst zal voor de ene gebruiker soms een verklaring in SAML en soms een verklaring in OAuth moeten verstrekken, afhankelijk van de technische implementatie van de service waarvoor geauthenticeerd moet worden. Een dienstverlener zal voor de autorisatiebeslissing de ene keer met SAML en de andere keer met OAuth moeten werken.

16. Bent u het eens met de constateringen en conclusies van de expertgroep inzake het open standaardisatieproces? [paragraaf 3.2 van het expertadvies]?

Aanvullend op de internationale standaardisatie zal er een beheerorganisatie moeten komen voor het lokale toepassingsprofiel.

17. Bent u het eens met de constateringen en conclusies van de expertgroep inzake het draagvlak? [paragraaf 3.3 van het expertadvies]?

Vanuit de techniek en de behoefte van gebruikers geredeneerd kan een zekere noodzaak voor het regelen van het toepassingsgebied van deze standaard worden beargumenteerd. We zien echter ook dat het beleidsmatig en bestuurlijk draagvlak voor een andere standaard dan SAML op dit moment er mogelijk niet is, zeker als dat buiten lopende programma's gebeurt.

18. Bent u het eens met de constateringen en conclusies van de expertgroep inzake de bevordering van de adoptie door opname op de lijst? [paragraaf 3.4 van het expertadvies]?

Opname van de internationale standaard zonder meer bevordert adoptie niet en zou zelfs contraproductief kunnen werken omdat er geen overeenstemming is over de interpretatie is, zie ervaringen met SAML. Opname van een goed doordacht en afgestemd toepassingsprofiel zou dat wel kunnen doen.

Vragen over hoofdstuk 4 van het expertadvies
("Adoptieactiviteiten")

Vraag:
19. Bent u het eens met de adoptie-aanbevelingen van de expertgroep aan het Nationaal Beraad Digitale Overheid? [hoofdstuk 4 van het expertadvies]

Zie het antwoord op vraag 1.

Resterende inhoudelijke opmerkingen

Vraag:
20. Is/zijn er volgens u nog andere informatie of overwegingen die aan het Forum en Nationaal Beraad Digitale Overheid zou moeten worden meegegeven voor een besluit over het opnemen van deze standaard op de 'pas toe of leg uit'-lijst?

Als eerder al genoemd: ontwikkel een standaardprofiel voor de toepassing van RESTful APIs dat integraal beschrijft hoe de Nederlandse overheid communicatie, beveiliging en techniek op basis van een aantal onderliggende standaarden inricht.

3. Reactie Belastingdienst

Van: Feijen, B (Bruun) (IVB)
Verzonden: maandag 20 maart 2017 13:26
Aan: Forum standaardisatie
CC:
Onderwerp: RE: Openbare consultatie over standaarden voor websitebeveiliging, API-autorisatie en elektronische handtekeningen

Lancelot
Hierbij de reactie van de belastingdienst. Bij vragen kan je contact opnemen met mijn collega Maurice Laarhoven.

1. Bent u het eens met het advies van de expertgroep om Oauth2.0 met een 'pas toe of leg uit'-verplichting op te nemen op de lijst met open standaarden nadat er een gemeenschappelijk toepassingsprofiel is ontwikkeld? Ja, eens.
2. Zijn er volgens u in deze aanvullingen of anderszins wijzigingen nodig in paragrafen 1.5, 'samenstelling expertgroep' (bezien vanuit het doel van de procedure om zoveel mogelijk belanghebbende te betrekken)? Nee, niet nodig
3. Bent u het eens met het door de expertgroep geadviseerde functionele toepassingsgebied? [paragraaf 2.1 van het expertadvies]?Ja, eens
4. Bent u het eens met het door de expertgroep geadviseerde organisatorische werkingsgebied? [paragraaf 2.2 van het expertadvies]? Ja, eens
5. Bent u het eens met de constateringen en conclusies van de expertgroep inzake de toegevoegde waarde? [paragraaf 3.1 van het expertadvies]?ja, eens
6. Bent u het eens met de constateringen en conclusies van de expertgroep inzake het open standaardisatieproces? [paragraaf 3.2 van het expertadvies]?ja, eens
7. Bent u het eens met de constateringen en conclusies van de expertgroep inzake het draagvlak? [paragraaf 3.3 van het expertadvies]?ja, eens
8. Bent u het eens met de constateringen en conclusies van de expertgroep inzake de bevordering van de adoptie door opname op de lijst? [paragraaf 3.4 van het expertadvies]?ja, eens

Met vriendelijke groet

Bruun Feijen
CIO-Office