Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Logius

Contactpersoon
Alexander Green (vz.)
T 06 2146 4182
Alexander.Green@logius.nl

Lizzy Wellink (secretaris)
T 06 2531 0240
Lizzy.wellink@logius.nl

Datum
22-10-2024

Kenmerk

Verslag Technisch Overleg OAuth

Vergaderdatum en tijd: 10 oktober 2024
10:00-11:00 uur

Vergaderplaats: Logius- zaal Oranje 7.045 en via Webex

Deelnemers

Leden	Departement	Leden	Departement
Ad Gerrits	VNG	Koos Boersma	Geonovum
Alexander vder Woude	KvK	M Adema	Wetterskipfryslan
Andre vd Ouweland	Den Haag	Marcel vden Brink	KvK
Arnoud Quanjer	VNG	Martin Borgman	Kadaster
Bob te Riele	RVIG	Paul Dam	Lexdigitalis
Erwin Reinhoud	Kennisnet	Rob Ulrich	Amsterdam
Edward van Gelderen	VNG	Ronald Coenen	Tilburg
Erwin Willemsen	Enable-U	Ronald Koster	VNG
Frank Terpstra	Geonovum	Reinier Filé	Min IenW
Frits Bouma	OCW/DUO	Frank van Es	Logius
Geri Wolters	Ecosys	Bas Kooij	Productiehuis
Hans Oostrom	Waternet		
Heiko Hudig	Enable-U	Peter Haasnoot	Logius Standaarden
Hans Hendrikman	RVIG	Martin van der Plas	Logius Standaarden
Henk van Maanen	Aceworks	Edwin Wisse	Logius Standaarden
Henri Korver	VNG	Alexander Green	Logius Standaarden
John Zwart	RvdK	Lizzy Wellink	Logius Standaarden

Aanwezig:
(11 personen) Alexander Green (Logius)(vz), Bas Kooij (Logius), Hans Hendrikman (ipv Bob te Riele RvIG), Heiko Hudig (Logius), Erwin Reinhoud (Kennisnet), Andre van den Nouweland (gem Den Haag), Peter Haasnoot (Logius), Martin van der Plas (Logius), Nil Barua (Logius), Stas Mironov (Logius), Lizzy Wellink (secretaris Logius).

Afwezig (met berichtgeving):
Paul Dam, Ronald Coenen (laatste helft)(Tilburg), Martin Borgman (Kadaster), Frank Terpstra (Geonovum), John Zwart, Heiko Hudig, Marcel Adema, Frits Bouma, Koos Boersma, Erwin Willemsen, Rob Ulrich (gem Amsterdam), Arnoud Quanjer

1. Opening & mededelingen (vz)

Hartelijk welkom namens de voorzitter Alexander Green – Logius Standaarden, bij het Technisch Overleg OAuth.

- We starten kort met een voorstelronde, waarvan de personele mededelingen vanuit het Gegegevensuitwisselingsteam zelf zijn: tweetal nieuwe collega's zijn gestart: Nil Barua (per 1-9-2024) en Stas Mironov (per 1-10-2024). Edwin Wisse heeft het team verruild per 1-9-2024 voor de Ned. Peppolautoriteit (NPa).

Geen aanvullingen vanuit de TO-leden op de agenda Overleg/OAuth/2024-10-10 at main · Logius-standaarden/Overleg (github.com)
Als reactie op een vraag: Dit overleg is niet ter vervanging van het Kennisplatform API's beveiligingswerkgroep. De volgende werkgroep zal via Frank Terpstra worden georganiseerd. Dit overleg is het Technisch Overleg en heeft het mandaat tot het nemen van besluiten, elk TO-lid heeft stemrecht.

Mededelingen (Martin vd Plas)

- Samenvattend is OAuth versie 1.1. goedgekeurd door het TO d.d. 9 juli 2024, daarna ingebracht bij stuurgroep van het Kennisplatform en die hebben aangegeven dat ze er geen expliciet besluit over hoeven te nemen omdat versie 1.0. al eerder is goedgekeurd en op de PTLU-lijst staat opgenomen. De wijzigingen in versie 1.1. zijn ingebracht bij het MIDO Programmeringstafel Toegang en staat deze 29 oktober a.s. op de agenda. De notitie die daarvoor is ingediend is publiek ook beschikbaar. Als sluitstuk zal versie 1.1. ook aan het Forum voor Standaardisatie voor publicatie op de PTLU-lijst worden aangeboden.
  Gezien de status waar versie 1.1. zich in bevindt kan erop anticiperend gebruik worden gemaakt van deze versie.
- Nordic API's event (in Stockholm) met veel aandacht voor OAuth en security rondom API's – verslag zal worden gedeeld **<Martin vd Plas>.** O.a. API online leerportaal, toolset van Curity (https://oauth.tools), online security portal (https://apisecuniversity.com), FAPI2 financiële standaard (https://openid.net/wg/fapi/specifications/) plus nog collega's van Centric en AXway. Misschien op het KP-API de nieuwe standaard FAPI en de ontwikkelingen delen.

2. Issue met milestones versie 1.2.

9 open issues
Opmerkingen:

- Rfc 8705; OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound Access Tokens en PKI-Overheid certificaten #35. Martin Borgman
- Het tweede issue, use case uitbreidingen, is eigenlijk dubbelop, staan doorverwijzigingen in naar andere issues waardoor ze samengevoegd kunnen worden **<actie: Martin vd Plas>**

- In een sessie op het API-Kennisplatform waar de roadmap 2025 is besproken en als gebieden voor development werden gekozen door de zaal; DPoP (proof of possession) (is niet alleen een token synchrone keypair maar ook asynchrone versleutelingen toepassen), en neigt naar 1e issue mutual tLS als tweede onderwerp, en de wallet technologie (vanuit EU en is een draft). Vanuit het TO geen verdere interesse op wallet technologie vooralsnog.
- Slide ter begeleiding. Verduidelijking verschil tussen DPoP en mTLS, wordt door Heiko Hudig gedaan -extra token dat je meestuurt met je access-token en een nieuwe token/header welke bewijst dat je rechtmatige eigenaar bent verstuurd uit de client. Alternatief zou mtLS zijn maar opschalen moeilijk omdat je ook proxy's hebt, dus DPoP is schaalbaarder. DPoP maakt het flexibeler algemeen en ook flexibelere architectuur aan de client-kant. Een ander mechanisme is mtLS i.c.m. rfc 8705 waarbij je met de mtLS verbinding een access-token genereerd. Als server moet je dit ondersteunen. Fundamentele vraag, toepassen van dit soort technologie, ja wenselijk maar neemt complexiteit en extra werk met zich mee en partijen al dan niet aan OAuth willen beginnen. Wat vinden TO-leden hiervan? Structureel willen toepassen?
  Stemming vraag aan TO-leden, keuzes:
  - Als structurele toevoeging, overall toepassen
  - Voor het meer gelaagde model. Basisprofiel maken en een strong security profiel. Sowieso in DigiD en eHerkenning etc hebben we te maken met meerdere beveiligingsniveaus.

  Besluit: Meerderheid stemmen voor het meer gelaagde model.

- Vraag (Erwin): We hebben eerder naar iGov en FAPI gekeken en daar zijn beide standaarden ook in opgenomen en daar laten ze het een optie. Aansluiten op iGov en participeren in doorontwikkeling. Maar niet de tempo's parallel. Dan maar een rework als we op een nieuwe release moeten aansluiten.
  Antwoord (Heiko): Onze voorstel is om ook als optie neerzetten voor DPoP zodat je een advanced optie hebt. De ene optie rfc8705 of de andere optie DPoP. Je behandelt het als standing zeg maar. DPoP toevoegen. In de inleidend document welke use cases welke advanced security opties gekozen moeten worden.
  Anders nog in hoofdstuk 5 plaatsen, options, en bij iGov aansluiten als zij een wijziging maken.

3. Issue zonder milestones versie 1.2. (Heiko Hudig)

8 open issues

- We behandelen de issues weer a.d.h.v. de presentatie (Heiko Hudig) op het scherm, daar staan ook de andere profielen in. Feitelijk, een standaard die ook besproken is rich autorisation request (RAR) op de client, i.p.v. OAS scope als een heel werkgebied of ketenproces zoals payment of account overview, of dat je ook een kleinere goedkeuring bewerkstelligd. Een step-up autorisatie op de client voor bijvoorbeeld toepassingsgebied bij het ondertekenen van stukken.
  Je kunt ook losstaand, traditioneel voor identiteiten, maar toe te passen als 'represent attribute' tussen leverancier en overheidsinstelling. Vanuit OAuth server en niet vanuit client applicatie.

- Functioneel bekeken. Verantwoordelijkheid centraal voor het goedkeuring van transacties. Relatie met Toegang en OIDC, dat je die in lijn wil hebben. Ter toelichting OIDC is altijd een aanvulling op de OAuth, de rich autorisation request doe je uit de naam van een persoon (bv geautoriseerd voor goedkeuringen voor 5.000 euro, rich autoristation request (RAR) kan middels een pop-up de user de bedragen erboven toestaan waarmee ook meteen de ondertekenaar bekend is met naam en toenaam). Maar wat is de relatie met het OIDC profiel wat bij FvS goedgekeurde standaard is, en hoe verhouden de standaarden zich tot elkaar?
  We gaan in beide documenten een aanpassing doen en ook dat is een puzzel waar het dan terecht komt in beide documenten, met in het inleidend document waar terug te vinden is waar de samenhang dan zit. Een uitdaging zogezegd. Komt neer op het

structureren van de autorisatie attributen.
<actiepunt Heiko, Martin> documentatie op orde
<actiepunt> Erwin als reviewer opnemen net als Martin Borgman (deze laatste wil ook uit deze specificatie een aparte werkgroep voor dit onderdeel organiseren).
RAR in 1.2. opnemen of later bv 1.3?

- Twee rfc's die we nog kort doornemen, crossed advice single-sign-on (Heiko),
  1) voor een QR inlogmechanisme met rfc 8628 en ook nog
  2) een pushindicatie mechanisme met client initiated backchannel authentication (CIBA), dus dan kun je meer gebruik maken van mobile apps/devices om simpeler in te loggen. Als je denkt dat is een toepassing voor ons gebied dan is dit er een die we kunnen prioriteren.
  Deze staat voor versie 1.3. op de lijst.

- En dan nog de volgende use case token exchange rfc 8693 (Heiko).
  Presentatie delen met TO OAuth, plaatje verduidelijkt waarbij de client applicatie misschien een token heeft en de bevraging is richting een andere applicatie. Voor ons eigen domein heb je een andere autorisatie nodig. Als basisregistratie biedt je aan token gestructureerd met RAR of eigen claims, inwisselen van een token.
  Vraag van Hans Hendrikman, over basisregistratie en inwisselen van een token.
  Voorbeeld Justitie hebben al een API call, loggen in met een persoonlijke access token (persoonsgegevens), dit mechanisme zou voordelen bieden voor grote infrastructuur.
  Tussen basisregistratie en embedded info, te traceren en dan is er zekerheid ingebouwd en is de vertrouwensketen verzekerd.
  Op procesniveau als keten uit te schrijven. In de werkgroep Orkestratie, als over meerdere organisaties API aan gaat roepen, aantal use cases
  1) over een hele keten heen,
  2) tussen organisaties en
  3) binnen je eigen organisatie voor token exchange.
  <actiepunt> Behoefte aan procesbeschrijvingen, over meerdere organisaties heen over API token exchange. Genoeg aanknopingspunten om deze binnen versie 1.2 op te pakken.

  Een derde constructie binnen de basisregistratie binnen RvIG 'de bewerkersconstructie' dat betekent dat er een partij al autorisatie-houder is en een andere partij namens die partij op diens autorisatie een bewerking doet op de basisregistratie.
  <actiepunt Hans H.> Plaatje/beeld zoals RvIG als basisregistratie wordt geraadpleegd door vertegenwoordiger rondsturen. Zo'n dergelijk claim, zelfde claim zit al OIDC en dan heet het 'claim represent'. Bv leverancier namens de gemeente.

  Ter afsluiting van dit onderdeel, oproep namens de voorzitter om op de issues te reageren (in Github).

4. Roadmap - heden t/m Q4 2025

Issues
Op Github is deze roadmap opgenomen, als project. (Github: orgs/Logius-Standaarden/Projects/2) Backlog · ROADMAP API Access standaarden (github.com)

- Martin high priority is al behandeld en loopt. Use case voor Oauth.
- Drafts staan er ook in waar issues voor zijn aangemaakt. De use cases zijn opgenomen in de repository.
- Relatie met SAML en eHerkenning/SSOO Rijk. Ook SAML naar OAuth vertaling staat ook op de roadmap. Gaat om de technische vertaling maar ook de inhoudelijke vertaling. De KvK heeft dit nagevraagd en hun gebruikers uit verschillende domeinen geven meer/minder zekerheid afhankelijk van het domein over de identiteit zekerheid/identity assurance. Identity assurance meegeven door OIDC toe te voegen. Komt de identiteit van eIDAS, uit DigiD of eHerkenning is er niks aan de hand maar er

zijn verschillende betrouwbaarheidsniveau's denkbaar. In het kader van Know your Customer -KYC wel noemen.

Om dit onderwerp behapbaar te maken zullen we splitsen;
1) eerst een inleiding schrijven voor het issue om hem in een inleidend document op te nemen (verplichting om identiteit van hun klanten te verifiëren en gegevens te bewaren)
2) en dan wachten tot de specificatie formeel is, en op de backlog een tweede item opnemen zodat ie op de langer termijn formeel wordt opgenomen.
Een voorbeeld die tot de verbeelding spreekt, bv. in de zorgsector en het onderwijs, door simpel inloggen met een app crossed device single sign on, zodat het makkelijker wordt voor de zorgverleners (rfc 8628) of door de specificatie te volgen en dan kan het met de redirect.
Zijn er nog meer usecase onder de TO-leden of niet? Graag reageren op api@logius.nl of op Github.

5. *Rondvraag en afsluiting*

- Geen

Sluiting van de vergadering 11:00 uur.

Volgende vergadering staat gepland voor 9 januari 2025 van 10:00-11:00 uur
Het overleg zal online (via MS Teams/Webex) plaatsvinden. De agenda van het overleg zal doorgaans ruim een week vooraf worden rondgestuurd. Ook kunt u agendapunten die u mist of wil inbrengen mailen naar api@logius.nl

6. *Extra: Refinement issues (zonder milestone) die nog openstaan sinds vorige vergadering in juli 2024:*

- iGOV-profiel afkomstig uit de financiële wereld en dan zou een tekstvoorstel helpen om het aan versie 1.2. te hangen. Heiko Hudig en Martin Borgman **<Actiepunt Martin vd Plas, inplannen van een dagdeel om dit te borgen>** niet aan toe gekomen
- Open ID Connect en iGOV wat het zijn en hoe het bij iGOV zit plus de relaties leggen. **<actiepunt Martin vd Plas>** samenhangende set voor nieuwe versie 1.2. schrijven. Zal Martin nog aandacht aan besteden

Datum/nr	Omschrijving	Verantwoordelijk	
1104/02	Toetsing of er sprake is van Excellent beheer bij het Forum Standaardisatie. Navraag doen.	Martin van der Plas	O
1104/03	Wijzigingsvoorstel Heiko Hudig raakt tekst van iGov. Issue ook aanmaken bij iGov is een mooi initiatief aangezien zij er wat mee kunnen.	Heiko Hudig	O
1104/04	Staan nog twee issues op naam van Frank van Es, even nagaan of deze in versie 1.1. horen	Martin van der Plas	X
0907/05	Meest actuele versie van de release wordt gepubliceerd, uiterlijk 12 juli laatste op- en aanmerkingen	All	X
0907/06	iGOV-profiel afkomstig uit de financiële wereld en dan zou een tekstvoorstel helpen om het aan versie 1.2. te hangen. Heiko Hudig en Martin Borgman, Martin vd Plas. (dagdeel plannen)	Martin vd P, Martin Borgman, Heiko Hudig	O

0907/07	Open ID Connect en iGOV wat het zijn en hoe het bij iGOV zit plus de relaties leggen. Ergo samenhangende set voor nieuwe versie 1.2. schrijven.	Martin vd P	O
1010/08	Issues met milestones waarvan er dubbelop zijn naar één issue terugbrengen.	Martin	
1010/09	RAR documentatie op twee plekken op orde (incl inleiding)	Martin, Heiko	
1010/10	Use case token exchange rfc 8693 - Behoefte aan procesbeschrijvingen, over meerdere organisaties heen over API token exchange. Genoeg aanknopingspunten om deze binnen versie 1.2 op te pakken.	Heiko	
1010/11	Plaatje/beeld zoals RvIG als basisregistratie wordt geraadpleegd door vertegenwoordiger rondsturen	Hans Hendrikman	