



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

11-4-2024

Kenmerk

Verslag Technisch Overleg OAuth

Vergaderdatum en tijd

11 april 2024
10:00-11:00 uur

Vergaderplaats

Logius- zaal Oranje 6.047 en via MS Teams

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:

(17 personen) Alexander Green (Logius)(vz), Bas Kooij, Jeroen Mol, Hans Oostrom, Erwin Willemsen, Erwin Reinoud, Andre van den Nouweland, Ronald Coenen, Martin Borgman, Ronald Koster, Marc van Andel (Kadaster), Frank Terpstra, John Zwart, Jan Jaap Zoutendijk, Dennis de Geest, Heiko Hudig, Jeroen Mol, Martin van der Plas, Lizzy Wellink (secretaris Logius).

Afwezig (met berichtgeving):

Peter Haasnoot, Edwin Wisse, Marcel Adema, Frits Bouma, Rob Ulrich, Hans Hendrikman, Geri Wolters, Arnoud Qvanjer, Paul Dam,

Verzoek tot aanvullingen: gemeente Tilburg en DUO

Vanuit Gemeente Tilburg, heeft Ronald Coenen verzoek tot aanmelding Dennis de Geest en Sander de Kok willen toevoegen als deelnemers.

Frits Bouma (DUO) heeft Jeroen Bakker /ICT-architect en Marijn van Tiel /software-architect bij DUO aangevraagd als deelnemer.

1. Opening & mededelingen (vz)

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

Martin van der Plas (Logius) start met de aanleiding voor dit overleg, dat het inmiddels een jaar geleden is dat het TO OAuth door Logius is georganiseerd. API Design Rules versie 2.0. heeft de aandacht binnen Logius opgeëist maar is nu opgeleverd en dat betekent nu dat we meer aandacht aan OAuth kunnen geven. Uitgangspunt voor de genodigdenlijst was de werkgroep Security van het Kennisplatform API's en is mogelijk nog onvolledig.

- Er is een aardig aantal issues in de tijd opgespaard en gesorteerd en deze zullen we vandaag langslopen.
- Er is ook een aantal issues die we hebben klaarstaan voor de releases 1.1 en behandelen we hierna in het tweede deel van de vergadering.

Mededelingen:

- Alexander Green zal het voorzitterstokje van Martin (Gegevensuitwisselingsteam Logius) overnemen. Lizzy Wellink zal als secretaris in de ondersteuning voorzien.
- Vergadercyclus 11 april 2024, di 9 juli 2024, do 10 oktober 2024 en do 9 januari 2025. De overleggen zullen online (via MS Teams/Webex) plaatsvinden. De agenda van het overleg zal doorgaans ruim een week vooraf worden rondgestuurd. Ook kunt u agenda-punten die u mist of wil inbrengen mailen naar api@logius.nl.
- OpenID Connect is opgenomen op de pas toe leg uit lijst. Zie ook <https://www.forum-standaardisatie.nl/open-standaarden/authenticatie-standaarden>

BESLUIT: Om OpenID Connect standaard mee te nemen in dit overleg (bij geen bezwaar is dit unaniem aangenomen). We hebben het hier over authenticatiemechanisme via Single Sign On. We zullen de ontwikkelingen op dit gebied volgen en als vast agendapunt opnemen in dit overleg.

Martin vervolgt met voor de beeldvorming is de voorgestelde werkwijze dat we in het Technisch Overleg vooral besluiten nemen en formele zaken afhandelen en dat er in de werkgroep van het Kennisplatform API's aan inhoudelijke ontwikkelingen en aandachtspunten blijft gewerkt worden.

Het iGov -profiel dient als basis voor dit profiel. Vanuit iGov zijn er ook wekelijks overleggen waar je bij kan aanhaken als dat interessant is.

Werkversie: <https://logius-standaarden.github.io/OAuth-NL-profiel/>

2. Issuelijsten

Link delen in de notulen, pull request lijst: [openid / igov / Pull requests — Bitbucket](https://bitbucket.org/openid/igov/pull-requests/) of <https://bitbucket.org/openid/igov/pull-requests/>

We nemen de lijst door, van de Pull Request lijst wordt twee issues gewerkt: [#34](#) en [#39](#). Vervolgens rfc8705 Frank Terpstra vraagt of Jeroen Mol namens RWS het issue op zijn naam kan zetten. Rfc9068, Martin Borgman veranderen in Jeroen Mol.

De grootste wijziging is het toevoegen van de client credentials flow. Verder is de introductie uitgebreid met (visuele) toelichting van de use cases client credentials flow en de authorization code flow. De verschillen met iGov zijn duidelijker weergegeven: toevoegingen zijn in gekleurde blokken en van zaken die buiten scope beschouwd worden is de tekst rood en doorstreept.

De release zullen we beschikbaar stellen eerst voor een review en dan voor de publieke consultatieronde. Deze punten worden ingebracht in de Stuurgroep van het Kennisplatform API en daarna door naar het MIDO (Meerjarige Infrastructuur Digitale Overheid). En uiteindelijk door naar het Forum voor Standaardisatie voor de PTLU-lijst.

<Actiepunt Martin>: Komende weken. Release candidate klaarzetten dan via mail reviewen en bekijken. Afsproken is dit in zijn geheel via de mail te behandelen; de wijzigingen en actualiseringen die we hebben doorgevoerd, en de review daarop. (en niet middels een tussenliggend overleg nog voor 9 juli a.s.)

Werkafspraken -> Voor versie 1.1. gaan we de client credentials flow door voor de release. Voor de 1.1. versie zouden we excellent beheer moeten aanvragen of hebben we die al, toetsing wordt gedaan bij het Forum voor Standaardisatie.

<Actiepunt Martin>: navraag op dit punt doen.

Werkafspraken -> Voor versie 1.2., de vragen rondom versie 1.2. zijn al behandeld. Terugkijkend zijn er al een aantal correcties doorgevoerd. Staan nog 5 issues open. De behandeling van de lijst met issues wordt gedaan aan de hand van milestones die eraan gekoppeld zijn. Resultaat: staan 5 issues open, 11 closed.

Dringende zaken die nog meegenomen moeten worden in 1.2. uitbreidingen en actualiseringen.

- OpenID Connect wordt hierin meegenomen.
- De uitwerking van de POC (Proof of Concept) en hierin verder komen.

Vraag: zijn er nog andere dringende zaken die meegenomen moeten worden in deze release?

Checkvraag van Frank, nu de FSC update/discussie loopt via het Technisch Overleg Digikoppeling, en daarmee 'pending' is, komen de puzzelstukken dan straks allemaal bij elkaar? Reactie: Daar wordt wel vanuit gegaan. Bijvoorbeeld geldt dat ook voor het stuk client authentication van Heiko (rfc8705). Erwin voegt daar een vraag aan toe of de mailwisseling aangaande de 'dependency' op het uitbrengen van de client credentials (DUO) wordt meegenomen. Of het compatible is, want er wordt meer afgeweken misschien dan wat mogelijk is.

Dit laatste punt is bij nacheck eerder doorgestreept maar wordt nu op de client credentials lijst weer meegenomen en wordt van 'must' naar 'should' meegenomen in de 1.1. versie.

<Actiepunt?>: Wijzigingsvoorstel Heiko raakt tekst van iGov. Issue ook aanmaken bij iGov is een mooi initiatief aangezien ze er wat mee kunnen.

<Actiepunt Frank Terpstra>: En ook Frank maakt tweemaal een actiepoint aan voor de mail van Jeroen Mol en deze van DUO.

3. Bestaande issues (staan opgelijnd voor de versie 1.1.)

- Staan nog twee issues op naam van Frank van Es, even nagaan of deze nog gelden <actiepunt Martin>. In elk geval of deze in de versie 1.1. thuishoren.
- De vraag van Ronald Koster is net behandeld. Wordt al gecorrigeerd.
- Rfc8705, Heiko Hudig, staat op de agenda.

4. Komende releases versie 1.2. (vooruitkijken)

- Rfc 8705 (Heiko Hudig), mTLS vragen
- Uitbreiding use case met Heiko oppakken.

7 issues zonder milestones

- Van Edwin Wisse, goede uitleg maar we gaan het niet doorvoeren. Hier wordt een informatief document van gemaakt.
- Martin issue, ACR-claim toevoegen, deze was via de mail binnengekomen (jan 2023) maar maken we een nieuwe voor aan (april 2024).
- Issue van Jeroen Mol is ingediend, agenderen voor versie 1.2.
- Paragraaf 4.2. later op terugkomen
- De drie issues #16, #26, #36 aan elkaar koppelen in rfc9068 en naar versie 1.2. meenemen
 - Issue#25 behoorlijk technisch, geen herkenning in de groep. Aanbevelen of verplichten van response_mode = form_post
Aanbeveling goed overwegen. Dit issue staat al 2 jaar open (2 aug '22)
 - #16 Ghost account, is verjaard. Verwijzing rfc7519 en rfc9068 is hierop aanvullend.
Niet in de scope maar wel claims.
- Ad Gerrits niet aanwezig. Issue: Doel van standaard verhelderen. Toegelicht en gesloten tijdens TO.

5. Rondvraag

- Volgende week is er Security werkgroep, een groot gedeelte van deze groep treft elkaar dan weer.
- Informeren dat het Besluit is 'toepassen nieuwe versie beheermodel'.
- Oproep aan alle deelnemers om andere betrokken partijen voor dit TO OAuth uit te nodigen en dit door te geven/communiceren aan Logius - Lizzy Wellink.

Sluiting vergadering om 11:00 uur

Volgend TO OAuth zal plaatsvinden op 9 juli van 10:00-11:00 uur