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
20-01-2025

Kenmerk

Verslag Technisch Overleg OAuth

Vergaderdatum en tijd: 9 januari 2025
10:00-11:00 uur

Vergaderplaats: Logius- zaal Blauw 4.011 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), Heiko Hudig (Logius), Erwin Reinhoud (Kennisnet), Martin Borgman (Kadaster), Peter Haasnoot (Logius), Thomas Schellekens (Logius), Michiel Trimpe (VNG, i.p.v. Mark van Andel), 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), Frank Terpstra (Geonovum), John Zwart, Marcel Adema, Frits Bouma, Koos Boersma (Geonovum), Erwin Willemsen, Rob Ulrich (gem Amsterdam), Arnoud Quanjer (VNG), Bas Kooij (Logius), Bob te Riele (RvIG), Andre van den Nouweland (gem Den Haag), K. Boersma (Geonovum),

1. Opening & mededelingen (vz)

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

- We starten kort met een personele mededeling vanuit Logius, Standaarden Gegevensuitwisselingsteam, start van een nieuwe collega Tim van der Lippe per 1-1-2025 en hij geeft zelf een korte introductie met duiding op deelname aan het OAuth team en API Design Rules team.

Agenda wordt gevolgd zoals voorgesteld Overleg/OAuth/2025-01-09/tijdplan.md at main · Logius-standaarden/Overleg · GitHub.

- Samenvattend is OAuth 1.1. goedgekeurd in het MIDO *Gegevensuitwisseling*. Daarnaast zijn de wijzigingen in versie 1.1. ingebracht bij het MIDO Programmeringstafel *Toegang* d.d. 29 oktober. Als sluitstuk is versie 1.1. ook aan het Forum voor Standaardisatie (FvS) voor publicatie op de PTLU-lijst aangeboden. Bij FvS zal de doorloop ca 6-9 maanden zijn.
  Gezien de status waar versie 1.1. zich in bevindt kan erop anticiperend gebruik worden gemaakt van deze versie.
  De memo OAuth 1.1.Logius.pdf is ter naslag beschikbaar (Lonneke Scholten).
- Er wordt nu doorgewerkt aan versie 1.2., en vandaag behandelen we de wijzigingen voor deze versie (due juli 2025 = uitbreiding en actualisering).

Verslag van de vorige keer, d.d. 10-10-2024 is zonder verdere aanpassingen goedgekeurd.

2. Goedkeuringen wijzigingsvoorstellen OAuth (Martin van der Plas)

Behandeling 3 open issues:
Technisch inhoudelijk veel achtergrond beschikbaar per wijziging, de verzoeken tot wijzigingen zijn beperkt gebleven. Dank voor inbreng op pullrequests en graag blijven reageren.

Martin loopt de issues langs op het scherm middels een verduidelijkende presentatie met context en achtergronden:

- #68 Proof of Possession (POP/Demonstrating PoP) (is niet alleen een token synchrone keypair maar ook asynchrone versleutelingen toepassen). We praten hier over het Pullrequest #68. Ons wijzigingsverzoek fixt #65 en dat omschrijft Demonstrating PoP, en daar wilde we een laatste verwijzing naar rfc's op dat gebied bijwerken en zo het verouderde profiel updaten. Middels een branche 'rfc DPoP' zijn de wijzigingen doorgevoerd. In preview van DPoP, en dat is soms lastig te zien in .md, laat Martin op

twee schermen de twee versies zien om het verschil te tonen.
Toelichting: we hebben het over hoofdstuk 5, §5.1. eind van het document addendum waarin aanvullende beveiligingsmaatregelen worden benoemd. Het gaat om het aantonen van de eigenaarschap d.m.v. een private key.
We hebben de tekst aangepast, m.n. aantal zaken doorgestreept/doorgehaald:

1) een verwijzing naar active development bij het IEDF want deze is al afgerond;
2) Aangepast 'Variety of mechanism for doing this are outlined in the draft'… is geen draft meer en dus verwijderd uit het profiel;
3) Toevoeging bijvoorbeeld bij 'predicting hazard…. request ', is een verbijzondering die niet altijd passend is;
4) Toegevoegd DPoP met de rfc 9449, een extensie is hoe die techniek cryptografisch de verbinding verzorgd tussen het access token en de verbindende client. Samenvattend i.p.v. wat nog gaat komen in de variëteit in mechanismes hebben we hiermee de harde keuze gemaakt om rfc 9449 te volgen en toe te passen indien aanvullingen nodig.
5) Nog de toevoeging PoP tokens in 'SAML holder of key mechanisms …' eruit gehaald.
6) Nog de additionele content die we wel hebben aangepast omdat het niet meer in lijn met rfc 9449 zijn. Met het geven van deze context hopen we te verduidelijken;
7) als laatste verwijzen we nog naar meer gedetailleerde informatie over het veilig implementeren PoP, niet het standaardiseren maar het implementeren, dat is ook beschreven in de FAPI security profile, en daar willen we naar verwijzen.

We hebben de branch aangemaakt 'rfc DPoP'. Overzicht van rfc's en door 'files changed' kunnen we het volgen. In de div leesbaar.

Besluit: Wijzigingsverzoek door TO: Akkoord

- #69 Token exchange.
  Met dank aan Heiko Hudig zijn verschillende beelden van tokenexchange de vorige keer in september met het TO gedeeld en eerder al op een sessie in het Kennisplatform d.d. juni 2024. Tokenexchange tussen SAML en OAuth, in twee verschillende situaties, vanuit de client en vanuit de autorisation server zelf. Wat in de standaard staat is heel summier en met name ook een verwijzing naar andere rfc's. De intentie is om deze 'zachtere' beschrijvingen op te nemen in het Inleidend document. De daadwerkelijke wijziging is vrij summier gebleven. Staat in paragraaf 'Autorisationserver profile'. Tokenexchange grant type should be supported by the autorisationserver, en daarmee geven we een extra verplichting. Dat heeft impact. Maar om niet verdere toelichting op te nemen maar verdere uitwerking in best practises als betere oplossing zien. Met het ondersteunen van token exchange tussen OAuth tokens ook mogelijk, in verschillende situaties en in verschillende flows, terug te vinden in meer use cases.

Besluit: Wijzigingsverzoek door TO: Akkoord

- Issue #71, update van de autorisationserver en verplicht gebruik van PKIoverheid, fixes issue #70 betreft gebruik van keys, van de autorisation server maar is het mTLS verhaal en verplicht gebruik van PKIoverheid.
  - Ingaand op de feedback van Jan Jaap Zoutendijk, helaas niet aanwezig vandaag, in pullrequest opgenomen is één typo en dat de term 'could be used' niet geformaliseerd is. Dit laatste staat eigenlijk in een toelichting en is daarmee geen formaliteit. Dit zit ook in het autorisation profile, staat in §3.2.1. Enige wijziging blijft over in de additionele content die we al hadden. Wel belangrijk omdat we stellen dat in geval dat de autorisation server en de resource server niet opereren onder verantwoordelijkheid van dezelfde organisatie met weglating van de 'client' dat impact heeft want de situatie is natuurlijk dat het heel vaak zo is dat de client van de andere organisatie is. Dit is alleen relevant als je niet de eigenaar bent van de resource server en autoristation server. Ben je dat wel, dan is dit daarmee dus niet meer verplicht.
    - Versimpeling 'All caps zetten' wordt dan doorgevoerd (request van Jan Jaap Zoutendijk);

- ‘Each party’ is ook verwijderd want impliceert dat ook de client ook PKIoverheid certificaten moeten implementeren. Niet altijd relevant. Veel veiliger dan op tLS niveau alle partijen PKIoverheid laat implementeren.
  De focus is verschoven naar het signing van bearer token, omdat o.b.v. daarvan te achterhalen is welke organisatie jouw ID bevestigd. En daar hebben we dus de verplichting opgenomen dat je ook PKIoverheid moet toepassen want dan kan de signature worden getraceerd naar de authentieke overheidsorganisatie. En dus is dit veiliger en duidelijker.
- Laatste aanvulling is de laatste regel ‘Is de bearer token must be encrypted with a PKIoverheid certificate’ naast signing ook encryptie toepast dan moet dat dus ook met PKI overheid certificaat.

<Vraag van Erwin Reinhoud> Kan het implementatiedocument wat duidelijkheid stellen. B.v. Geen eisen stelt aan tLS koppelingen met n-points aan de autorisationserver en resourceserver t.a.v. het token, niet het n-point. Met OIN’s de partij identificeren. De overheidscertificaten voor de authenticatie, de server inzicht in de client maar de client kan niet het n-point identificeren.
Bewust gedaan omdat heel veel PKIoverheid certificaten kun je de private root bieden en met die private root krijgen de webclients een certificaat die ze niet accepteren. Van n-point tot n-point ligt in een ander domein, hoek Digikoppeling en FSC. (smalle scope)

Met dit OAuth profiel een hele brede scope waarbij verschillende types clients worden ondersteunen, we vooral helder willen zijn wat je zou moeten implementeren v.w.b. resourceserver en autorisationserver. Dan krijg je aanvullende vragen.
<O.b.v. de vragen vanuit DUO/OCW en Kennisnet> is deze context ook opgenomen in het ‘Inleidend document’? We moeten de samenhang in wijzigingen in iGov en de wijzigingen OAuth aangeven en daarnaast staan deze ook op de planning van de Roadmap.

3. Inleidend document (Martin van der Plas)

Algemene inleiding Open Authenticatie, de link is opgenomen Algemene Inleiding Open Authenticatie, in het kort het is nog een conceptversie, ruwe werkversie met alle onderwerpen rijp en groen door elkaar.
Wenselijk is om er nog meer structuur in aan te brengen. Een aantal segmenten opnemen naast de hoofdstukken.

- Eén segment over inleidende context, ter inleiding en verder welke video’s zijn interessant, welke stukken zijn beschikbaar, welke leveranciers,
- Daarna een segment met verdieping, wat beschrijven we nu eigenlijk over gebruik over mTLS en PKIoverheid,
- verdieping op het gebeid van orkestratie,
- Segment met best practices.

Issue aangemaakt voor de segmentering (Stas Mironov)
Daarnaast de uitnodiging aan de TO-leden om te reageren, aan te vullen, mee te lezen/reviewen. **<actiepunt TO-leden: Graag input/feedback>**

4. Roadmap - heden t/m Q4 2025 (Stas Mironov)

Op Github is deze roadmap opgenomen als projectboard (……) Backlog · ROADMAP API Access standaarden (github.com)
Op Kanban bord is publiek beschikbaar waarbij de uitnodiging is om te participeren. We willen de milestones beter bijwerken, en daarmee kan je de status beter aflezen hoever we daarin zijn.

De drie voorstellen zijn ‘in review’.

Open Issues Roadmap / Kanban-bord:

- #61 Bijvoorbeeld Opaque tokens staat 'in progress', staat ook klaar in het Inleidend Document, maar is dus ook tevens een van de use cases voor token exchange;
- #59 RAR (rfc 9396) opnemen in NL-Gov staat op Roadmap. Michiel van Trimpe wil graag op dit onderwerp aanhaken.
- Heiko legt uit, gaat om ondertekenen van een transactie, consent van een gebruiker, verantwoordelijkheid bij autorisation server, autorisation attribute wordt dan als token meegestuurd.
- #36 use case uitbreidingen (rfc 8628) SSO staan een aantal dingen in maar ook inlog QR-codes (zoals het binnenkomen bij een zwembad/bioscoop o.b.v. een verkregen QR-code als toegangsbewijs, aanwezigheidscontrole), dat is CIBA (Client Initiated Backchannel Authentication)
  Of: op een website ingelogd en dan volgt er een push notification op je mobile/client (voor gedistribueerde omgevingen)
- PAR pushed autorisation request, is een veiligere manier, redirect via een API en een URI terug (2.0. versie). Deze dient nog in OAUth ondergebracht te worden.

Presentatie Heiko Hudig <Link van de presentatie> die bij het KP-API is gegeven, daarin staat wat meer beschrijving van alle onderwerpen die Heiko net heeft opgesomd. Informatief voor alle TO-leden.

5. Rondvraag en afsluiting

- Heiko Hudig: reprensents claims
- Michiel Trimpe: interesse in RAR, haakt graag aan
- Martin Borgman: niet hoorbaar maar bv in de chat?
- Thomas Schellekens: neemt contact op met Stas over zijn vraag

Mochten er nog meer personen zijn die geïnteresseerd zijn om deel uit te maken van het Technisch Overleg OAuth kunnen zij zicht aanmelden via api@logius.nl, algemene mailbox van dit TO.

Hartelijk dank voor uw aanwezigheid en bijdrages. Sluiting van de vergadering 11:00 uur.

Volgende vergadering staat gepland voor 10 april 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

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	Martin vd P, Martin Borgman, Heiko Hudig	O

	Borgman, Martin vd Plas. (dagdeel plannen)		
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 heeft Lizzy uitgezet en nagevraagd maar is geen reactie meer opgekomen	
1010/12	N.a.v. 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.	Martin vd P is hier niet aan toegekomen maar zal dit z.s.m. oppakken.	
0901/26	**Besluit wijzigingsverzoek #68 Proof of Possession (POP/Demonstrating PoP): Akkoord**		B
0901/27	**Besluit wijzigingsverzoek #69 Token exchange: Akkoord**		B
0901/28	Inleidend document, graag feedback/input. NB. Is ook issue aangemaakt voor segmentering.	Alle TO-leden	O