Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Logius

Contactpersoon
Stas Mironov (vz.)
T 06 2525 9855
Stas.Mironov@logius.nl

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

Datum
23-10-2025

Kenmerk

Verslag Technisch Overleg OAuth

Vergaderdatum en tijd: 9 oktober 2025
10:00-11:15 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	Stas Mironov	Logius Standaarden
Henk van Maanen	Aceworks	Alexander Green	Logius Standaarden
Henri Korver	VNG	Lizzy Wellink	Logius Standaarden
John Zwart	RvdK		

Aanwezig:
(11 personen)(Stas Mironov Logius)(vz), Frank Terpstra (Geonovum, werkgroep Beveiliging), Jacob-Jan van Harten (Politie - Authenticatie), Tristan Smits (Politie – Integratie), Heiko Hudig (Logius – OIDC standaarden), Erwin Reinhoud (Kennisnet), Hans Oostrom (Waternet), Martin van der Plas (Logius – Toegang & Wallet), Tim van der Lippe (Logius), Alexander Green (Logius), Lizzy Wellink (secretaris Logius).

Afwezig (met berichtgeving):
Martin Borgman (Kadaster), Peter Haasnoot (Logius), Paul Dam, Ronald Coenen (Tilburg), John Zwart, Koos Boersma (Geonovum), Erwin Willemsen, Rob Ulrich (gem Amsterdam), Arnoud Quanjer (VNG), Bas Kooij (Logius), Bob te Riele (RvIG), André van den Nouweland (gem Den Haag), Frank van Es

1. Opening & mededelingen (vz)

Hartelijk welkom namens de voorzitter Stas Mironov – Logius Standaarden, bij het Technisch Overleg OAuth.

Mededelingen van de voorzitter:

- We starten kort met een voorstelrondje;
- Aansluitend personele mededeling vanuit Logius, Gegevensuitwisselingsteam Standaarden. Martin van der Plas is geen direct teamlid meer maar ondertussen in dienst getreden bij Logius als system architect bij ART Toegang en Wallet (T&W), Productiehuis. In die hoedanigheid en door betrokkenheid op de standaarden blijft hij bij dit Technisch overleg aangehaakt;
- Het vorige TO OAuth was d.d. 10-4-2025. Tussentijds is TO OAuth in afwachting van visievorming bij minBZK niet bijeen geweest en dit is het opvolgende TO;
- Van de domeinarchitect Toegang bij Logius (Diepak Atwaroe) vernomen dat DigiD vastzit aan verouderde koppelvlakken. Er komen updates aan vanuit domein Toegang. We worden meegenomen in de voortgang op uitfasering oude koppelvlakken. Dit impliceert uitfaseringsstrategie in een memo die we verwachten begin volgend jaar als ook OIDC versnelling – focus; **<actiepunt**> team GU Standaarden die een bijdrage leveren aan de strategie en de memo als discussiedocument;
- <Martin van der Plas> Domein Toegang Erik Snijder is verantwoordelijk. Ontwikkelingen stelsel Toegang die bij hem bekend zijn: Bouwstenen rondom bevoegdheidsverklaringsdienst machtiging, komt ook één voor wettelijke vertegenwoordiging bij als meerjarige of als wettelijke vertegenwoordiging (professionals);

Agenda
Agenda wordt gevolgd zoals voorgesteld Overleg/OAuth/2025-10-09/README.md at main · Logius-standaarden/Overleg.

Belangrijkste bespreekpunten vandaag:

1. Invulling voor multi-actor authorisation, de presentatie en delegatie. (presentatie, uit het OIDC profiel). De voorgestelde veranderingen of inrichting willen we graag bespreken;
2. Feedback van de politie op de technische documenten;
3. Vraag vanuit het Forum voor Standaardisatie om een herziening van het functioneel toepassingsgebied en hoe dit past in het gehele overheidsplaatje.

Verslag van de vorige keer, d.d. 10-4-2025 is stilzwijgend zonder verdere aanpassingen goedgekeurd.

2. Behandeling bespreekpunten OAuth (vz)

Behandeling (in willekeurige volgorde) zoals de leden van het TO aanbrengen:

Ad 2) Feedback vanuit de Politie op de technische documenten;
A.d.h.v. de mail van Tristan Smits Politie.
-Client Credentials grant type 3.1.3. conflicterend en niet machine-to-machine, autorisation code flow. Inhoudelijke aanvullingen zijn verwerkt. Oppakken met iGov.
-Ciphers verouderd voor het beveiligen van data? In principe is met verwijzing naar de NCSC richtlijnen, (nieuwe versie, update in alle werkversies documenten), voldoende afgedekt. Oppakken met iGov.
-Er staat een Pullrequest genaamd 'verwerkte feedback' open. Commentaar mag nog toegevoegd worden. En uiteindelijk kan worden gemerged en in de toekomstige versie worden gepubliceerd (na verkrijging 'Uitstekend beheer').
-Naast zinsbouw verbeteringen ook een aantal inhoudelijke zaken zoals DPoP en FSC. Dit is een bruggetje naar het volgende bespreekpunt.

Ad 3) Vraag vanuit Forum om het huidige functioneel toepassingsgebied te herzien;
Toepassingsgebied n.a.v. Het expertadvies OAuth 2.0. van auteur Paul Dam (Forum lid) stamt uit 2016/17. Document Expertadvies-OAuth2.0.pdf.
www.forumstandaardisatie.nl/sites/default/files/2020-7/Expertadvies-OAuth2.0.pdf

> Citerend uit NL-Gov profile OAuth 2.0.: 'Moet worden toegepast bij applicaties waarbij *de gebruiker (vertaling van 'users')* of resource owners impliciet of expliciet toestemming geven aan een dienst van derden om namens deze toegang te krijgen tot gegevens via een REST API waarvoor ze het recht van toegang hebben'.

Tijdens de intake versie 1.2. is door het Bureau Forum voor Standaardisatie gewezen op gebruik van hetzelfde toepassingsgebied. Hoe interpreteren jullie deze opmerking?
<Frank Terpstra>, input allereerste versie ca 6 jaar geleden. Uit zijn hoofd betrof het in beginsel een rechtendelegatie en autorisatie, is uiteindelijk 'toegang' geworden, maar niet client credentials flow bijvoorbeeld. Maar algemeen wil hij graag het toepassingsgebied 'breder' hebben.
<TO-leden> Toepassingsgebied tussen Ov-Ov en semi-overheden is de standaard. Maar is de uitbreiding Client credentials flow ook opgenomen? OAuth altijd toepassen op REST API met een aantal uitzonderingssituaties. Zowel users als machines in het profiel willen terugzien. Namelijk daar waar FSC ophoudt? Er zijn overlappingen met Digikoppeling. Digikoppeling is voor sectoroverschrijdend verkeer. Toepassingsgebied nog updaten tussen Ov-Ov. 'Beveiligen' of 'toegang' opnemen in de tekst, waaruit blijkt dat verbinding tussen twee systemen beveiligd is. Òf mTLS, of OAuth of Open.
In hoofdstuk 5, beweging richting sender constraints tokens, staat mogelijkheid mTLS, DPoP (Demonstrating PoP) als advanced security option, kun je zien als equivalent.
Naar elkaar toe kunnen trekken, rechtendelegatie en client credentials flows, FSC OAuth compliant maken. Voor het beveiligen van REST API's voorkeur voor OAuth.

Beslisboom: https://github.com/Logius-standaarden/OAuth-NL-profiel/issues/126
(Stas toont sheet op het scherm daar waar de Politie een update op beslisboom had gedaan, want eerdere versie leek meteen na FSC een API aan te bieden maar zou anders moeten) en is meest handige tool om door FSC en OAuth beslissingen heen te kunnen gaan, welke use-cases kom je daar tegen. Dit om een ambtenaar met een aanbesteding de juiste keuzes te laten maken.
<actiepunt> Beslisboom handig voor intern gebruik. Deze tool beschikbaar stellen.

Conflict tussen interpretatie toepassingsgebied vanuit TO Digikoppeling of vanuit TO OAuth, het Forum interpreteert het waarschijnlijk naar machine-to-machine FSC, met personen OAuth. Maar tevens in het geval OAuth óók voor machine-to-machine.

<Frank Terpstra> Volgens mij vraagt het Forum voor Standaardisatie, hoe kunnen we het huidige werkingsgebied aanpassen vanuit de gebruiker gezien? Je biedt een API aan. Nu we alle mogelijkheden bekeken zijn de opties:
1) Je hebt Open Data waar niets aan beveiligd hoeft te worden;
2) API aanbieden waarvoor beveiliging nodig is. Waar je wel met OAuth kan werken voor toegang en rechtendelegatie aan een derde (zonder mTLS);
3) FSC van Overheid-Overheid waar mTLS wel nodig is.

- Een aantal heldere profielen stellen. Qua procedures best veel werk om aan te bieden.
- Voor de Politie als API gateway beheerder, niet één API, juist behoefte aan één soort standaard.
- Stap extra is beter de lading te dekken wat er nu in het NL Gov gebied komt te staan, breder. Client credentials flow erbij. Dichterbij de praktijk en haalbaar.

<Besluit> Vz stelt voor om FSC zoveel mogelijk hun profiel/standaard laten lijken op OAuth standaard om niet verschillend technisch in elkaar te zitten (dezelfde soorten tokens te gebruiken). Dit impliceert dat er met FSC afstemming dient te komen (conflict oplossen van de system-to-system) en dan het functionele toepassingsgebied aanpassen.
En daarnaast terugkoppelen aan het Forum voor Standaardisatie dat dit de gekozen weg is en dat je een helder toepassingsgebied definieert. Impliceert niet slechts een papieren exercitie.
Opmerking: OIDC/Europese standaard wordt voorkeur aangegeven vanuit de overheden. M.b.t. toepassingsgebied. Moeten we hier rekening mee houden?

<Actiepunt> Vz stelt voor om verder over te praten. 1) Eigen voorstel doen per stakeholder. 2) En hoe zouden we het moeten verduidelijken? Daar ziet iedereen de voordelen van. Zonder je te laten beïnvloeden door FSC.

3. *RAR toelichten (Heiko Hudig)*

Use cases voor: Rich Authorization request (RAR, rfc9396) · Issue #59 · Logius-standaarden/OAuth-NL-profiel

Voorzitter doet een introductie op dit onderwerp. Wij zijn begonnen met een bijlage te schrijven, omdat customer represents claim nu in het OIDC profiel stond. Wij vonden niet per se dat het daarin thuishoorde en kregen we ook nog een vraag om die standaard OAuth te maken. Heiko heeft een voorstel gedaan met een fictieve use-case en Stas heeft de vorm gedaan hoe het eruit zou kunnen komen te zien als bijlage.

Heiko Hudig deelt zijn scherm. Aanleiding van het verhaal is een represented party en representation claims standaard in het ID-token en access-token staan. Maar in feite zijn dat niet-standaard tokens. Dan is RAR misschien meer passend.

Rich Authorisation Request is een brede standaard die je kan toepassen als een scope onvoldoende is. Specifieke token voor een bepaald doel. Dat kan zijn dat een bepaalde delegatie van bijvoorbeeld een gemeente (verantwoordelijke partij), kan ook zijn als bijvoorbeeld een bepaalde transactie, d.w.z. iets wat je wil goedkeuren dan kan je RAR gebruiken. Scope niet voldoende maar scope als werkgebied zou moeten interpreteren, aangifte, inentingen, parkeerbeheer, etc.
In het geval van delegatie met FSC is een specifiekere autorisatie en kan je (uitgegeven token) autorisatie attributen in meegeven, dit doe ik in het kader van een bepaalde gemeente.
Dit is zoals het eruit zou kunnen zien. Dit is mijn voorstel. Dit is een generieke manier waarop je het kan doen.
Een alternatief zou zijn tokenexchange, twee verschillende tokens die je omzet naar één token.
De eerste past beter en meer generiek bij de delegatie claim die nu in FSC zit.

Authorisation details bij de Politie wil je meegeven. Heeft deels overlap met AuthZen en aanvulling op elkaar. Moet nog afgestemd worden met Michiel Trimpe.
Dank aan Heiko Hudig voor zijn presentatie.

4. Rondvraag en afsluiting

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

Hartelijk dank voor uw aanwezigheid en bijdragen. Sluiting van de vergadering 11:10 uur.

Volgende vergadering staat gepland voor 13 januari 2026 van 10:00-11:15 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	
110424/02	Toetsing of er sprake is van Excellent beheer bij het Forum Standaardisatie. Navraag doen.	Martin van der Plas	G
090724/07	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
101024/10	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	
090125/28	Inleidend document, graag feedback/input. NB. Is ook issue aangemaakt voor segmentering.	Alle TO-leden	G
091025/29	Domein Toegang, verouderde koppelvlakken punt, team GU Standaarden die een bijdrage leveren aan de strategie wat in een memo komt als discussiedocument;	Logius	O
091025/30	Update Beslisboom (van Politie) wordt beschikbaar gesteld, handig voor intern gebruik.	Stas	O
091025/31	Op functioneel toepassingsgebied de verduidelijking zoeken. 1) Vraag aan stakeholders om hun idee te delen? 2) Hoe zou je je het moeten verduidelijken (zonder beïnvloeding FSC)	Logius	O
091025/32	Functioneel toepassingsgebied. Afstemming met FSC m.b.t. conflicterend aspect machine-to-machine, verduidelijking/uitbreiding naar zowel users als machines (standaarden zoveel mogelijk op elkaar laten lijken)	Logius/Stas	O