Memo

Aan
Sander Loos, Bob van der Staak, Bram de Graaf, Jan-Maarten Verbree, Reinout van Rees, Geri Wolters, Flip Dirksen, Erik de Rooij, Stef Hummel

Datum	**Kenmerk**	**Aantal pagina's**
25 juli 2017	11200534-DSC-0014	2
Van	**Doorkiesnummer**	**E-mail**
Stef Hummel	+31(0)6 1019 8112	stef.hummel@deltares.nl

Onderwerp
Verslag bijeenkomst Authenticatie/Autorisatie bij de DD-API

Verslag van de meeting over authenticatie en autorisatie bij de DD-API
(Meeting bij Hydrologic, Amersfoort. Aanwezig: zie 'Aan')

RWS heeft gevraagd in welke mate de DD-API-specificatie voldoet aan de de API-strategie van de DSO (Digitaal Stelsel Omgevingswet – De DD-API zou een kandidaat kunnen zijn voor een deel van de door het "Informatiehuis Water"[1] te bieden services).
In grote lijnen is dit zeker het geval, al zijn er op details een aantal verschillen.
M.b.t. het onderwerp van de vergadering is het belangrijkste punt uit deze API-strategie: de DSO gaat OAuth2 gebruiken. Stef zal het API-strategie-document naar een ieder mailen.
(Zie ook nog enkele opmerkingen over de DSO aan het eind van dit verslag.)

Bob geeft een presentatie over OpenID Connect als mogelijke laag op OAuth2.
Tijdens de presentatie wordt regelmatig gediscussieerd over de diverse aspecten die de revue passeren.
Belangrijk punt daarbij is het beheer van de groepen gebruikers. Hydrologic en EcoSys voelen ervoor om de groepen centraal te beheren, maar Nelen & Schuurmans heeft de ervaring dat die complex kan worden wanneer verschillende gebruikers in verschillende groepen zitten.

Na Bob's presentatie, die Hydrologic's visie op authenticatie/autorisatie beschrijft (dus ook die van Sander en Bram), volgt een rondje langs de ander partijen. (Zeer) Korte samenvatting:

- Geri (EcoSys):
  Auth2 is een prima keuze, OpenID Connect wellicht ook. Graag het beheer (groepen en rollen) centraal
- Erik (Deltares):
  Deltares wil er naartoe dat men 'aan de buitenkant' op maar één manier binnenkomt, waarna men op basis van z'n id wel of niet bij diverse systemen mag. Vergelijkbaar dus met wat we in de Digitale Delta beogen
- Flip (RWS):
  Intern wordt ActiveDirectory gebruikt; mensen van buiten komen via E-herkenning binnen. OpenID Connect past hier goed bij
- Reinout/Jan-Maarten (Nelen & Schurmans):
  Benadrukken nog eens het beheersaspect. Hoe ga je om met de potentiële veelheid en verwevenheid van groepen?

---

[1] Dit "informatie-huis" levert de aan water gerelateerd informatie t.b.v. van de Omgevingswet. Niet te verwarren met het huidige IHW.

Besloten wordt om nader kennis te nemen van elkaars aanpak. Dit leidt tot het volgende ‘huiswerk’:

- Nelen & Schuurmans verdiept zich nader in de aanpak van Hydrologic
- Vice versa: Hydrologic verdiept zich nader in de aanpak van Nelen & Schuurmans
- Beide partijen vergelijken de aanpak van de andere partij met hun eigen aanpak, en houden beide systemen tegen het licht van de eisen t.b.v. de Digitale Delta
- Ze rapporteren hun bevindingen. Geri neemt deze rapportages door als ‘reviewer’
- Flip zal navragen wat de motivatie is bij de DSO om niet naast OAuth2 ook nog b.v. OpenID Connect te nemen
- Stef zal onderzoeken wat voor de Digitale Delta de meerwaarde is van OpenID Connect naast OAuth2

Vanwege de zomervakantie wordt volgende bijeenkomst pas over zes weken gehouden. Een ieder heeft dan voor en/of na zijn vakantie tijd om zich nader in de materie te verdiepen.

Enkele punten uit het gesprek van Flip en Stef met Tony Sloos, domeinarchitect Informatie & Kernfuncties bij de DSO:

- *Bij de DSO wordt OAuth2 gebruikt voor autorisatie, en DigiD en E-herkenning voor Authenticatie*
- *Er wordt binnen de DSO een eigen identity-provider ingericht, die niet buiten de DSO gebruikt kan worden.*
- *OpenID Connect wordt niet gebruikt, omdat de overheid geen gebruik wil maken van grote identity-providers als Facebook en Google*
- *De attributen die bij OpenID Connect in het token mee gaan worden binnen de DSO opgevraagd bij een ‘attribute-service-provider’*
- *Uit een API-specificatie wordt documentatie gegenereerd, waaronder een schema voor de json-response.*
  Het lijkt erop dat we de DD-specificatie beter om kunnen zetten naar OAS 2.0 (Open API Specification, voorheen Swagger 2.0), omdat daarvoor blijkbaar meer tooling is. (Stef heeft al even gekeken naar automatische conversie van RAML naar Swagger, en daar zijn (gratis) tools voor. Maar overgaan heeft pas zin als we ook de overgang van het testen – nu gebaseerd op Postman/RAML – geregeld hebben).