digiGO digitaal samenwerken in de Gebouwde Omgeving

DSGO Afspraken over toegang tot data

Samenvatting discussiepunten

Datum
15 juni 2023

Betreft
Tech-Xperiment werkconferentie DSGO

Locatie
Postillion Hotel Bunnik

Tijd
09:00 – 16.00

Aanwezig waren medewerkers van de volgende organisaties:

Ambrero Software, Asset Wise, Bakker & Spees B.V., Balance & Result Organisatie Adviseurs, BIM Base, BIM Loket, Cadac Group, Compano Software, CROW, digiGO, EIFFEL B.V., Horizon Internet Technologies, IMAGEM, IRP, Ketenstandaard, Madaster, SPIE Nederland B.V., SPOTinfo, TBI, VDNDP, Waternet, WEM No-Code & Witteveen+Bos

Discussiepunten:

N.B. onderstaande samenvatting geeft de kern van de discussie en brainstorm tijdens de bijeenkomst weer en heeft nog geen besluitvormend of –sturend karakter. Ze is daarmee uitsluitend bedoeld als startpunt voor verdere uitwerking en discussie.

1. **Maakt het DSGO gebruik van OpenAPI en/of andere open source componenten?**

Ten behoeve van schaalbaarheid maakt het DSGO zoveel mogelijk gebruik van open standaarden, zie hiervoor de pagina richtinggevende principes. De huidige APIs zijn gebaseerd op een OpenAPI specificatie.

2. **Hoe gaat het DSGO zorgen voor een goede API-documentatie ten behoeve van implementatie en snelle ontwikkeling?**

Parallel aan het afsprakenstelsel wordt er gewerkt aan een developer portal als een van de voorzieningen. Voorzieningen zijn ondersteunde faciliteiten bij implementatie en gebruik van het DSGO. Oplevering van een MVP developer portal en MVP test tool staat gepland voor Q2 2024, zie voor meer informatie de pagina aanpak ontwikkeling DSGO.

3. **Voorziet het DSGO verschillende levels voor informatiebeveiliging om toetreding laagdrempeliger te maken?**

Op dit moment voorziet het DSGO een enkel niveau voor informatiebeveiliging als basis voor het veilig en betrouwbaar data delen binnen deze sector. Als vanuit concrete gevallen blijkt dat er andere levels nodig zijn, kan dat overwogen worden. Daarbij geldt wel dat verschillende levels van informatiebeveiliging een extra laag complexiteit in het stelsel creëert, wat implementatie juist kan vertragen of de interoperabiliteit in het ecosysteem kan verlagen. Wanneer dit onderwerp wordt behandeld zal deze afweging worden gemaakt.

4. **Hoe werkt authenticatie van personen in het DSGO?**

Op het moment zijn er nog geen afspraken over de authenticatie van personen opgenomen. Afspraken hierover worden mogelijk in volgende versie(s) uitgewerkt, en zullen zoveel mogelijk gebaseerd zijn op iSHARE en zo open standaarden zoals bijvoorbeeld OpenID Connect volgen.

5. **Wat zijn de implicaties voor deelnemers van de onweerlegbaarheidseisen?**

Om waardevolle data vertrouwd te delen is het vanuit juridisch perspectief belangrijk dat de datadienst response onweerlegbaar is. Het DSGO gebruikt hiervoor gesigneerde JWTs in de HTTP header, met in de JWT payload een verwijzing (hash) van de HTTP body op basis van ETSI standaard TS 119 182-1. Om onweerlegbaarheid aan te tonen moeten partijen zowel de HTTP headers als de HTTP body opslaan, zie voor meer informatie de pagina JSON Web Tokens (JWT).

6. **Wat zegt het DSGO over de levensduur van JWTs?**

Het DSGO eist dat JWTs 30 seconden geldig zijn, voor meer informatie zie de pagina JSON Web Tokens (JWT).

7. **Waarom voorziet het afsprakenstelsel meerdere door de markt geleverde autorisatieregisters?**

Autorisatieregisters worden door de markt ontworpen om innovatie en een passend aanbod te stimuleren, o.a. omdat autorisatieregisters specifieke kenmerken kunnen hebben afhankelijk van de use case of deel van de keten waar ze opereren. Daarnaast heeft niet elke use case een autorisatieregister nodig omdat er niet altijd wordt gewerkt met delegaties. Ook is dan nog niet altijd een autorisatieregister nodig voor de opslag van delegaties, dit kan ook bij de rechthebbende of bij de datadienstaanbieder.

8. **Wat zijn de gevolgen voor de datadienstaanbieder als er verschillende autorisatieregisters zijn waar delegaties van de rechthebbende staan opgeslagen?**

Op dit moment zijn de eisen vanuit het DSGO aan autorisatieregisters nog niet bekend, zie deze pagina voor meer informatie over de aanpak voor ontwikkeling van het DSGO.

9. **Wat biedt het DSGO voor het regelen van autorisaties binnen de organisatie? (Bv persoon X van bedrijf Y mag bij deze data, maar collega's van bedrijf Y niet)**

Afspraken over de technische implementatie van fijnmazige autorisaties van personen binnen organisaties zijn momenteel nog niet opgenomen in het afsprakenstelsel. Het onderwerp fijnmazige autorisaties wordt in toekomstige versies ontwikkeld.

10. **Wat zegt het DSGO over het beschikbaar houden van (oudere versies van) datasets en het beschrijven hiervan in het resource endpoint?**

Op het niveau van generieke afspraken worden in het DSGO geen eisen gesteld aan de beschikbaarheid van data- en versie management. De DSGO stelselcatalogus, een van de toekomstige stelselvoorzieningen, faciliteert een mechanisme om hierover te communiceren. Het is de verantwoordelijkheid van de datadienstaanbieder om in de datadienstdefinitie op te nemen wat de beschikbaarheid is van een datadienst met optioneel een versienummer inclusief datum, mocht dat relevant zijn voor de datadienst in kwestie.

11. **Hoe kunnen partijen zich binnen het DSGO identificeren als zowel de datadienstaanbieder als de datadienstgebruiker gebruik maakt van een SaaS-oplossing?**

Organisaties die gebruik maken van een SaaS-oplossing (en niet de leverancier van de oplossing) moeten zich met een EORI-nummer identificeren en met een eIDAS certificaat kunnen authentiseren. Als een deelnemer van het DSGO gebruik maakt van een SaaS-oplossing is het de verantwoordelijkheid van de deelnemer om te voldoen aan het DSGO, en om met de SaaS-leverancier de benodigde vereisten af te stemmen. De deelnemer aan het DSGO is uiteindelijk verantwoordelijk om zich aan de afspraken in het stelsel te houden.

12. **Wordt het mogelijk via GraphQL data te delen in het DSGO?**

Op het moment zijn alle datadiensten binnen het DSGO op basis van RESTful APIs. Het gebruik van GraphQL kan hieraan worden toegevoegd als hier behoefte aan is. Zie de pagina aanpak ontwikkeling van het afsprakenstelsel voor meer informatie.

13. **Wat zegt het DSGO over de levensduur van access tokens?**

Het DSGO stelt dat access tokens, maximaal 3600 seconden geldig zouden moeten zijn. Zie hiervoor de pagina POST /token.