digitaal samenwerken in de Gebouwde Omgeving

Samenvatting discussiepunten

Datum
29 november 2023

Betreft
DSGO Publieke review: Technisch

Locatie
Youmeet (Orteliuslaan 11, 3528BA Utrecht)

Tijd
13:00 – 16:00

Bij de technische review waren medewerkers van de volgende organisaties aanwezig:

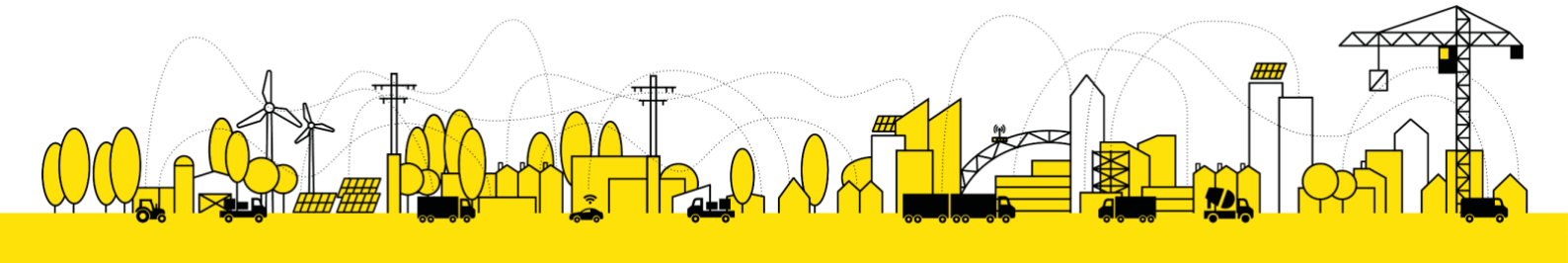
Cadac, CROW, Dutch Data Masters, NVTB en Rijksvastgoedbedrijf

Discussiepunten

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

In de functionele review zijn vragen gesteld over het nut van specifieke conceptafspraken in het DSGO. Wat is de conclusie van die discussie?
Om in een specifiek geval tussen twee partijen data te kunnen delen moet over elk aspect (van elke bit van de API specificaties, en de exacte betekenis van wat er wordt uitgewisseld tot elke letter van de procesbeschrijving en contracten) duidelijkheid bestaan. Het DSGO legt in ieder geval generieke conceptafspraken vast, maar faciliteert daarnaast (op verzoek van de sector) de totstandkoming van specifieke conceptafspraken, daar waar nuttig en gewenst. De behoefte om specifieke afspraken in het DSGO op te nemen is bovendien in de sector op bestuurlijk niveau uitgesproken en daarmee een van de doelen van het DSGO. Voor meer informatie zie de pagina Aanpak ontwikkeling van het afsprakenstelsel DSGO.

De generieke conceptafspraken van het afsprakenstelsel, welke fungeren als basis, laten ruimte en keuzevrijheid aan partijen bij de invulling van de datadienst voor elke specifiek geval. Deze keuzevrijheid geeft partijen de mogelijkheid om een datadienst naar eigen voorkeur in te richten. Tegelijkertijd zorgt meer keuzevrijheid voor minder standaardisatie en daarmee minder schaalbaarheid van het DSGO. De schaalbaarheid van het DSGO kan echter verhoogd worden door de keuzevrijheid in te perken door middel van specifieke conceptafspraken. Specifieke conceptafspraken werken aanvullend op de generieke conceptafspraken en gelden altijd voor een gedefinieerde context in de sector, en moeten partijen die buiten die context handelen niet beperken.
Samen met de markt wordt in de verdere ontwikkeling van het afsprakenstelsel bepaald wat de juiste balans is tussen de keuzevrijheid en opstellen van specifieke afspraken/standaardisatie. Bovendien worden door de markt geadresseerde risico's rondom specifieke conceptafspraken (bijvoorbeeld het abrupt wijzigen van specifieke afspraken) behandeld in werkgroepen om die risico's zoveel mogelijk te mitigeren.



digiGO digitaal samenwerken in de Gebouwde Omgeving

Samenvatting discussiepunten vervolg

Betreft
DSGO Publieke review: Functioneel

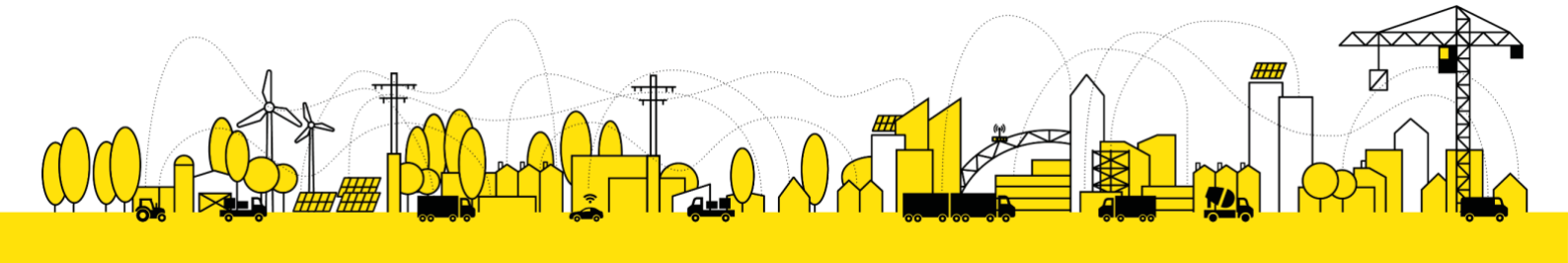
Betekent het richtinggevende principe kostenefficiëntie dat het DSGO afspraken gaat maken over het besparen van kosten?
Nee, de richtinggevende principes zijn geen scopebepalingen, maar geven richting bij het maken van keuzes over de inhoud van het afsprakenstelsel. Het afwegen van keuzes betreft afspraken kan lastig zijn omdat het complexe materie betreft, waarbij veel keuzes zowel voor– als nadelen kennen. De richtinggevende principes fungeren meer als een kompas dan als harde eisen bij het kiezen voor bepaalde afspraken.

Het richtinggevende principe kosten efficiënt stuurt op dat het afsprakenstelsel kostenefficiënt dient te zijn. Het gaat daarbij om de kostenefficiëntie van het gebruik en het beheer van het afsprakenstelsel. Keuzes die in het afsprakenstelsel gemaakt worden, moeten zo min mogelijk tot extra kosten leiden. Uiteraard altijd in afweging met de andere richtinggevende principes. Voor meer informatie zie de pagina Richtinggevende principes.

Is het de verantwoordelijkheid van de datadienstaanbieder om het autorisatiebeleid technisch te implementeren?
De datadienstaanbieder is de partij die verantwoordelijk is voor de datadienst, inclusief het opstellen van het autorisatiebeleid en het nemen van een autorisatiebesluit. Om een autorisatiebesluit te nemen moet de datadienstaanbieder de autorisatie-informatie toetsten tegen het autorisatiebeleid. Hoe de datadienstaanbieder dit doet is buiten scope van het DSGO. Voor meer informatie zie de pagina Autorisatie.

Kan het autorisatiebeleid van een data object met verloop van tijd veranderen?
Het autorisatiebeleid wordt opgesteld voor datadiensten en niet voor data objecten. Data objecten kunnen na verloop van tijd binnen meerdere organisaties bestaan en meerdere datadienstaanbieders kunnen een datadienst aanbieden met daarin een bepaald data object (productinformatie kan zowel belangrijk zijn bij het ontwerp en gedurende het beheer van assets). Bovendien is het aan een datadienstaanbieder om het autorisatiebeleid op te stellen en optioneel te wijzigen, dit is buiten de scope van het DSGO. Voor meer informatie zie de pagina Autorisatiebeleid opstellen.

Hoe federatief is het DSGO in werkelijkheid als partijen ook data kunnen opslaan, waardoor data niet altijd bij de bron blijft?
In praktijk is het niet gewenst, gebruikelijk en haalbaar dat data te allen tijde bij de bron blijft. Zo is het in praktijk gebruikelijk om een ontwerp van gebouw na oplevering over te dragen aan een asset manager. Bijvoorbeeld om de afhankelijkheid naar partijen die data duurzaam beschikbaar moeten houden te beperken of omdat brondata voor de inrichting van systemen en processen niet zonder meer optimaal is.
Het DSGO wil de mogelijkheid bieden om controle te houden over data die bij andere partijen opgeslagen wordt om een federatief ecosysteem te faciliteren. Zo kan data gedeeld worden onder een licentie dat het bijvoorbeeld niet toegestaan is data verder te delen of te bewerken. Zie de pagina Juridische bepalingen voor meer informatie.



digiGO digitaal samenwerken in de Gebouwde Omgeving

Samenvatting discussiepunten vervolg

Betreft
DSGO Publieke review: Functioneel

Waarom wordt er in het DSGO gebruik gemaakt van certificaten?
Certificaten worden in het DSGO gebruikt voor meerdere doeleinden. Op transportniveau worden certificaten gebruikt om de datadienstaanbieder te authentiseren. Op datadienstniveau worden certificaten gebruikt om de datadienstgebruiker te authentiseren. Daarnaast worden certificaten gebruikt om ontvangen berichten onweerlegbaar vast te leggen. Zie de slides van de werkgroep en het afsprakenstelsel Authenticatie & Informatiebeveiliging voor meer informatie.

Waarom wordt er in het DSGO gebruik gemaakt van certificaten uitgegeven onder de eIDAS-verordening?
De eIDAS-verordening is een Europese verordening, deze verordening regelt de randvoorwaarden voor elektronische transacties in de Europese markt.
Met de onder eIDAS uitgegeven certificaten (QWACs en QSeals) kunnen partijen worden geauthentiseerd en transacties onweerlegbaar worden vastgelegd. Omdat de certificaten onder een Europese verordening zijn uitgegeven bieden deze voor hun doeleindes rechtszekerheid op EU-niveau. Bovendien is de overheid in transitie van PKIOverheid naar het gebruik van eIDAS certificaten voor gebruik in veilig digitale diensten (zoals een belastingaangifte). Het gebruik van certificaten uitgegeven onder de eIDAS-verordening wordt in de onderstaande vragen en versie v0.8 van het afsprakenstelsel verder toegelicht.

Kunnen QSeals net als API keys ook gebruikt worden om binnen een organisatie personen of bepaalde afdelingen te authentiseren en op basis daarvan toegang te geven tot datadiensten?
QSeals zijn gekoppeld aan een juridische entiteit en kunnen alleen gebruikt worden voor M2M datadiensten. Het is met QSeals niet mogelijk om individuen of afdelingen binnen een organisatie te authentiseren. Wanneer een organisatie specifieke individuen of afdelingen rechten wil geven om M2M datadiensten af te nemen kan ze haar eigen processen hierop inrichten. Indien de authenticatie van specifieke personen in de data uitwisseling van belang is, moet dit in de datadienst worden geregeld. Dit kan bijvoorbeeld middels eHerkenning. Dit wordt in een toekomstige versie van het afsprakenstelsel verder uitgebreid als H2M authenticatie. Zie de pagina Authenticatie voor meer informatie.

Gaat het DSGO het verplichten om datadiensten onweerlegbaar aan te bieden en af te nemen?
Wanneer (in de nabije toekomst) meer commerciële processen en beslissingen gebaseerd worden op data, wil je als partij zeker zijn dat gedeelde data wordt ontvangen zoals dat door de verzender bedoeld is. Bovendien wil je ontvangen data in het geval van een dispuut kunnen gebruiken als bewijslast. Hierom kan het nuttig zijn om datadienstverzoeken en/of responsen onweerlegbaar vast te leggen.

Het DSGO biedt een mechanisme om onweerlegbaarheid mogelijk te maken, maar laat de keuze of dit nodig is bij de datadienstaanbieder. Daarmee is het is aan de datadienstaanbieder om te bepalen of ontvangst van een datadienstverzoek en/of een datadienstrespons onweerlegbaar dient te zijn. Wanneer een datadienstaanbieder onweerlegbaarheid van het datadienstverzoek verplicht kan een datadienstgebruiker een datadienst niet afnemen als ze hier niet aan voldoet. Voor meer informatie zie de pagina Onweerlegbaarheid.

digiGO digitaal samenwerken in de Gebouwde Omgeving

Samenvatting discussiepunten vervolg

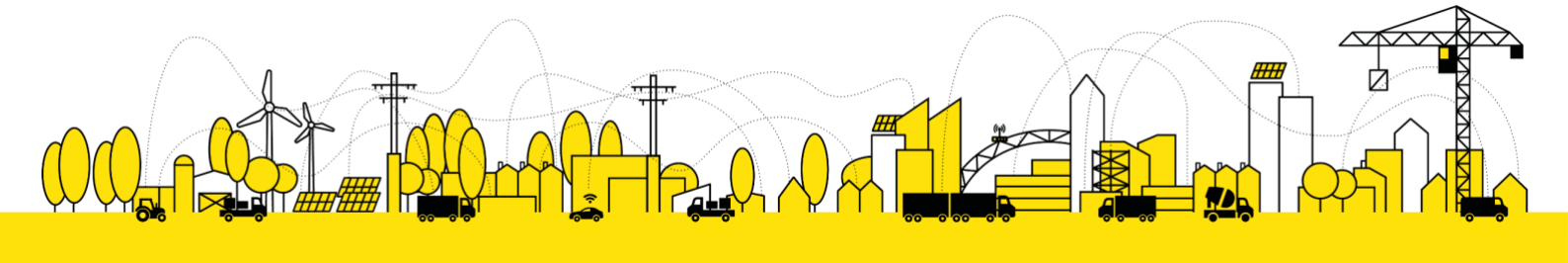
Betreft
DSGO Publieke review: Functioneel

Gaat het DSGO het verplichten dat verstuurde en ontvangen transacties, inclusief metadata worden opgeslagen?
Nee, dit is buiten scope van het DSGO. Het is aannemelijk dat datadienstaanbieders die besluiten een dienst aan te bieden waarvan ontvangst van het verzoek en/of response onweerlegbaar is vastgelegd, dit ook opslaan. Het is daarnaast aannemelijk dat datadienstgebruikers data, op basis waarvan zij commerciële besluiten nemen, opslaan. Wanneer data onweerlegbaar is ontvangen en opgeslagen kan hierop worden teruggevallen in het geval van disputen. Het is niet verplicht om ontvangen berichten op te slaan, hiermee gaat echter de onweerlegbaarheid van berichten verloren. Zie de pagina's Onweerlegbaarheid en JSON Web Tokens (JWT) voor meer informatie.

Kunnen de QWACs die voor authenticatie op transportniveau gebruikt worden ook gebruikt worden om onweerlegbaarheid te waarborgen?
QWACs zijn certificaten uitgegeven onder de Europese eIDAS-verordening. Technisch gezien is het mogelijk QWACs te gebruiken om onweerlegbaarheid te waarborgen. QWACs bieden net als QSeals een asymmetrische sleutel om berichten te tekenen. Echter is in de eIDAS-verordening bepaalt dat enkel QSeals binnen de EU rechtszekerheid bieden. QSeals worden onder andere voorwaarden worden uitgegeven dan QWACs en zijn hiermee juridisch gezien andere certificaten. Zie de pagina Ondertekening voor meer informatie.

Wat mag een datadienstbroker doen met data die zij door haar rol in bezit heeft?
De datadienstbroker is een (technisch) dienstverlener die mag optreden namens een datadienstgebruiker en/of datadienstaanbieder. Een datadienstbroker mag additionele diensten bieden die toegevoegde waarde leveren mits dit is overeengekomen met de partij namens wie zij optreedt (bijvoorbeeld inzichten creëren op basis van verschillende datadiensten die zij heeft afgenomen). Een datadienstbroker is niet het subject van autorisatie voor de afgenomen dienst. Daarmee mag een datadienstbroker geen datadiensten afnemen zonder overeenkomst met de datadienstgebruiker of datadiensten aanbieden. Zie de pagina Datadienstbroker voor meer informatie.

Kan een datadienstaanbieder valideren dat een datadienstverzoek van een datadienstbroker daadwerkelijk is geïnitieerd door, en uitgevoerd namens, een datadienstgebruiker?
Het mogelijk dat de datadienstaanbieder bij ieder datadienstverzoek van een datadienstbroker valideert of dit geïnitieerd is door een datadienstgebruiker. In praktijk wordt gebruik gemaakt van een datadienstbroker om datadienstgebruikers te ontlasten. Door bij een datadienstgebruiker te valideren of een broker namens de datadienstgebruiker optreedt nemen de lasten van een datadienstgebruiker toe en vermindert de toegevoegde waarde van de broker. Er zijn verschillende alternatieven om het risico dat de broker niet namens en geïnitieerd door een datadienstgebruiker optreedt te mitigeren. Een mogelijke maatregel is dat de datadienstbroker bij ieder datadienstverzoek een bewijslast meestuurt dat zij namens de datadienstgebruiker optreedt, of dat de datadienstaanbieder in de stelselcatalogus controleert of een broker namens een datadienstgebruiker mag optreden.



digiGO digitaal samenwerken in de Gebouwde Omgeving

Samenvatting discussiepunten vervolg

Betreft
DSGO Publieke review: Functioneel

Er zijn verschillende alternatieven om het bovengenoemde risico en andere risico's rondom de datadienstbroker te mitigeren. In de technische review was niet voldoende tijd om deze goed in kaart te brengen en af te wegen. In een volgende werkgroep of review wordt dit verder behandeld.

Het is gebruikelijk dat een datadienstbroker data opslaat, bewerkt en vervolgens deelt met een datadienstgebruiker, hoe gaat het DSGO om met risico's die hieruit ontstaan bijvoorbeeld gevolgen van beslissingen gebaseerd op foutieve data?
De risico's die bewerking van data door een datadienstbroker meebrengt zijn use case afhankelijk en moeten worden afgewogen tussen de datadienstbroker en de partij namens wie de datadienstbroker optreedt. In het DSGO kunnen afspraken komen die het vertrouwen tussen een datadienstbroker en de partij namens wie zij optreedt bevorderen (bijvoorbeeld over het archiveren van data). Dit moet verder worden onderzocht.