

Samenvatting discussiepunten

Datum
26 maart 2024

Betreft
Publieke Review Afsprakenstelsel DSGO: Technische review

Locatie
Youmeet, Utrecht

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

Tijd
13:00-16:00

Cadac Group, Gemeente Amsterdam, Homij, InterGarant Groep BV, KleurrijkWonen, Packhunt, Rijksvastgoedbedrijf, Schoots Architecten, Stichting kennisplatform CROW, VanMeijel, Vidomes.

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.

Waarom is de overeenkomst technische conformiteit geïntroduceerd naast de deelnameovereenkomst?

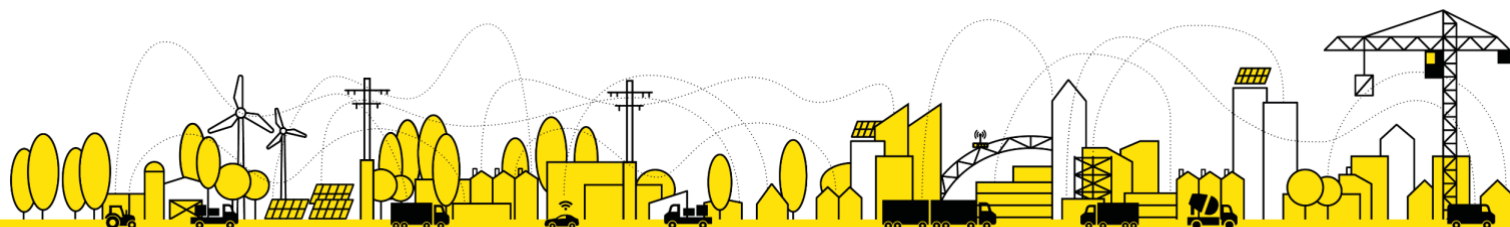
In de initiële opzet van het DSGO was er alleen een deelnameovereenkomst welke getekend wordt om deel te nemen aan het DSGO. Uit de sector ontvangen wij de feedback dat het voor veel partijen niet haalbaar is om op korte termijn de deelnameovereenkomst te tekenen. Wel geven dezelfde partijen aan dat ze graag steun uit willen spreken voor het DSGO of al wel op korte termijn technisch conform het DSGO kunnen handelen. Op basis van deze feedback is de overeenkomst technische conformiteit geïntroduceerd omwille van marketing en adoptie. Voor meer informatie zie [Overige overeenkomsten voor gebruikers](#).

Hoe verhoudt de overeenkomst technische conformiteit zich tot de deelnameovereenkomst?

De overeenkomst technische conformiteit is een overeenkomst bedoeld voor (toekomstige) datadienstaanbieders die een dienst hebben die technisch voldoet aan het DSGO. Hierbij wordt gecontroleerd of de datadienst conform het afsprakenstelsel functioneert, om de technische interoperabiliteit tussen partijen te borgen. Het verschil met de deelnameovereenkomst is dat een partij niet hoeft te voldoen aan (o.a.) de juridische en operationele aspecten van het DSGO, en geen recht heeft op inspraak in de governance van het DSGO. Deze verschillen maken de overeenkomst technische conformiteit voor partijen 'lichter' om te tekenen dan de deelnameovereenkomst.

Welke voordelen biedt een overeenkomst technische conformiteit voor ondertekenaars?

(Toekomstige) datadienstaanbieders die (nog) niet in staat zijn om volledig conform het DSGO te handelen als datadienstaanbieder, maar wel een datadienst technisch conform het DSGO willen aanbieden, laten zien technisch conform het DSGO te kunnen handelen. Hiermee wordt technische interoperabiliteit gerealiseerd. De overeenkomst technische conformiteit geeft deze partijen een manier om dit te communiceren.



Samenvatting discussiepunten vervolg

Betreft

Publieke Review Afsprakenstelsel DSGO: Technische review

Aan welke onderdelen moet een partij voldoen om een overeenkomst technische conformiteit te mogen tekenen?

Een getekende overeenkomst technische conformiteit verklaart dat de datadienst van een partij technisch voldoet aan het DSGO. Dit wil zeggen, dat de dienst aan (o.a.) generieke technische standaarden, API-specificaties, identificatie, authenticatie, autorisatie en de technische aspecten van informatiebeveiliging afspraken (zoals de beveiliging van verbindingen en berichten) voldoet. Het is de bedoeling dat de zogenoemde 'technisch conform datadienstaanbieders', voldoen aan de afspraken over het gebruik van het DSGO merk en de vindbaarheid van datadiensten. De afspraken over deze onderwerpen zijn belangrijke onderdelen van de marketing en adoptie van het DSGO en passen in het doel van de overeenkomst om de technische interoperabiliteit te garanderen met een zo 'licht' mogelijke overeenkomst.

Hoe gaat het DSGO zorgen dat de overeenkomst technische conformiteit niet een keurmerk op zich gaat worden wat de urgentie wegneemt bij partijen om te streven naar het tekenen van een deelnameovereenkomst?

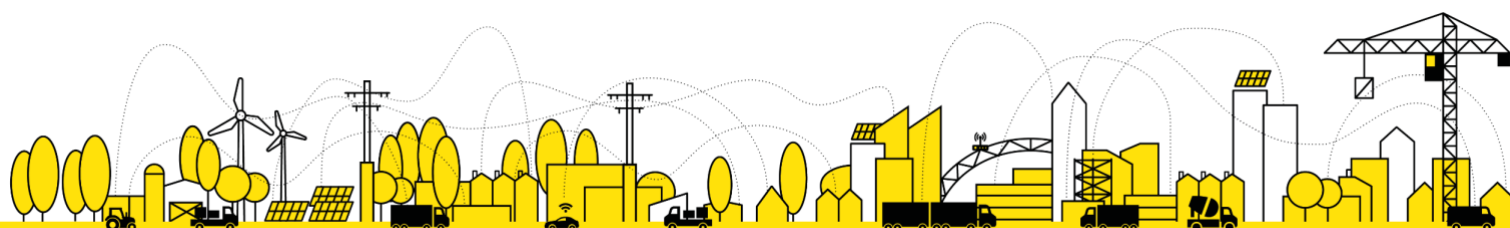
De overeenkomst technische conformiteit wordt in de communicatie gepositioneerd als een overeenkomst met aanzienlijk minder waarborgen dan de deelnameovereenkomst. De beperkingen van de datadienst van een partij die alleen een overeenkomst technische conformiteit heeft getekend, worden duidelijk gecommuniceerd richting de markt. Een partij die slechts technisch conformiteit kent, krijgt ook een apart logo voor de zichtbaarheid herkenbaarheid naar andere partijen. Daarnaast wordt het belang van de juridische afspraken, de operationele processen en de inspraak in de governance binnen het DSGO duidelijk gecommuniceerd.

Wie bepaalt welk betrouwbaarheidsniveau nodig is voor het authenticeren van menselijke gebruikers binnen een datadienst?

Het DSGO legt de keuze voor een authenticatieoplossing bij een datadienst bij de datadienstaanbieder voor het authenticeren van menselijke datadienstgebruikers. Een datadienstaanbieder mag kiezen welk betrouwbaarheidsniveaus verplicht is in haar datadienst, omdat het niet generiek te bepalen is hoe hoog het betrouwbaarheidsniveau van een authenticatieoplossing moet zijn. Om datadienstaanbieders hierin te ondersteunen heeft het Forum Standaardisatie een '[handreiking betrouwbaarheidsniveaus](#)'. Hierin kunnen datadienstaanbieders informatie zoeken voor het classificeren van het benodigde betrouwbaarheidsniveau voor datadiensten. Voor meer informatie zie [Betrouwbaarheidsniveaus](#).

Is het van belang dat het DSGO een authenticatie met hoog betrouwbaarheidsniveau eist voor datadiensten met menselijke datadienstgebruikers om de kwaliteit van het DSGO te borgen?

De verwachting is dat het DSGO in de toekomst een breed pallet aan datadiensten gaat bevatten. Daarom is ervoor gekozen om verschillende soorten betrouwbaarheidsniveaus voor de authenticatie toe te staan. De keuze voor een betrouwbaarheidsniveau ligt bij een datadienstaanbieder zelf waardoor een laag betrouwbaarheidsniveau enkel afstraalt op de betrouwbaarheid van die datadienst en niet van het gehele DSGO. Ook al is in de EU de trend naar hogere betrouwbaarheidsniveaus duidelijk zichtbaar, niet elke datadienst heeft een hoog betrouwbaarheidsniveau van menselijke datadienstgebruikers nodig, en daarom kan een datadienstaanbieder ervoor kiezen om bijvoorbeeld gebruik te maken van Microsoft login voor de authenticatie van personen. Voor meer informatie zie [Authenticatie](#).



Samenvatting discussiepunten vervolg

Betreft

Publieke Review Afsprakenstelsel DSGO: Technische review

Welke betrouwbaarheidsniveaus voor authenticatie van menselijke datadienstgebruikers kent het DSGO?

De huidige opzet voor de betrouwbaarheid van de authenticatieniveaus voor menselijke datadienstaanbieders in het DSGO is gebaseerd op de authenticatieniveaus uit de [eIDAS richtlijn](#), zoals volgt uit de '[Handreiking betrouwbaarheidsniveaus](#)' van het Forum Standaardisatie. [eHerkenning](#) maakt gebruik van meer betrouwbaarheidsniveaus. Tijdens publieke review kwam de wens naar voren om het EH2+ betrouwbaarheidsniveau uit eHerkenning aan het DSGO toe te voegen. Dit biedt een extra niveau tussen de eIDAS betrouwbaarheidsniveaus Laag en Substantieel, welke waardevol zou zijn voor datadienstaanbieders.

Is het mogelijk voor internationale partijen om datadiensten aan te bieden in het DSGO?

De belangrijkste beperking hiervoor is dat het DSGO nu niet volledig in het Engels beschikbaar is. Het DSGO volgt verder namelijk open standaarden die voor alle partijen makkelijk te gebruiken zijn. Hiermee is het in principe ook mogelijk voor internationale partijen om een datadienst aan te bieden volgens het DSGO.

Wat definieert een datadienst kijkend naar de technische implementatie en hoe verhoudt dat zich tot de toetreding van een datadienstaandbieder en vindbaarheid van de datadienst?

Een datadienst kan uit meerdere API-calls bestaan. Het zou niet zo moeten zijn dat elke aparte endpoint als aparte datadienst wordt beschouwd in de stelselcatalogus. Op dit moment maakt het DSGO gebruik van /capabilities endpoint, waarin features worden gedefinieerd als datadiensten. Dit wordt in toekomstige versies nog verder vormgegeven, maar het is de intentie dat een datadienst als feature meerdere endpoints kan gebruiken. Voor meer informatie zie [/capabilities](#).

Een datadienstaandbieder moet toetreden tot het DSGO, en bij het toetreden wordt gevalideerd dat de aangeboden dienst voldoet aan het DSGO. Wanneer een datadienstaandbieder vervolgens additionele diensten volgens het DSGO wilt aanbieden, wordt door de beheerorganisatie proportioneel bepaald of elke datadienst volledig gecontroleerd moet worden. De mate waarin dat nodig is, kan sterk afhangen van de situatie. Voor meer informatie zie [Toetreding](#).

Een datadienstspecificatie is complementair aan de Swagger documentatie van een datadienst. De datadienstspecificatie maakt datadiensten vindbaar in het DSGO, en bevat additionele informatie over de dienst zoals welke toegangscontrole regels van toepassing zijn of welke licenties gelden op data betrokken bij de datadienst. Voor meer informatie zie [Data service specification](#).

Wie nemen er zitting in de Change Advisory Board en de Gebruikersraad?

De samenstelling van het Change Advisory Board (CAB) en de Gebruikersraad bestaat uit de (toekomstige) deelnemers van het DSGO. Zowel de CAB, als de Gebruikersraad bestaat uit een vaste groep van de deelnemers om constante kennisopbouw en evenwichtige besluitvorming te borgen. Onder de CAB kunnen diverse werkgroepen plaatsvinden, afhankelijk van het ingebrachte onderwerp. De samenstelling van deze werkgroepen kan wisselen en wordt bepaald afhankelijk van de agenda (denk aan expertise/deelsectoren). Het is de ambitie om een goede



Samenvatting discussiepunten vervolg

Betreft

Publieke Review Afsprakenstelsel DSGO: Technische review

vertegenwoordiging van de gehele sector plaats te laten nemen in de CAB en de Gebruikersraad. Voor meer informatie zie [Governance](#).

Mocht je interesse hebben om plaats te nemen in de Change Advisory Board neem dan contact op met Jorrit Penninga (jorrit.penninga@digigo.nu). Hij is binnen het DSGO-programma verantwoordelijk voor het beheer en de governance van het DSGO.

