digitaal samenwerken in de Gebouwde Omgeving

Samenvatting discussiepunten

Datum
18 september 2023

Locatie
YouMeet (Utrecht)

Tijd
13:00 – 16:00

Betreft
Technische werkgroep DSGO

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

Cadac Group, Contakt Consulting, Hyrde, Kleurijk wonen, Rijksvastgoedbedrijf, SPIE, TBI, Techniek Nederland, VORM, Witteveen+Bos, Woonstad Rotterdam

Discussiepunten

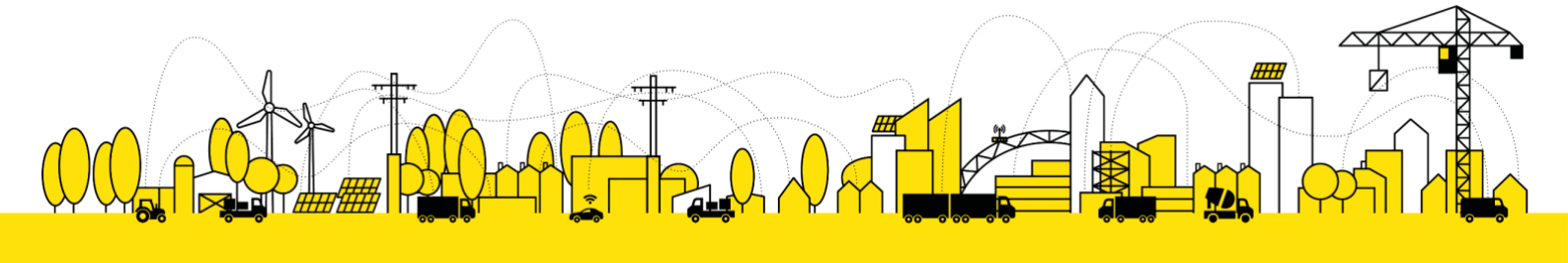
N.B. onderstaande samenvatting geeft de kern van de discussie tijdens de bijeenkomst weer en heeft nog geen besluitvormend of sturend karakter. Ze is daarmee uitsluitend bedoeld als startpunt voor verdere uitwerking en discussie.

Het DSGO is een initiatief voor de Nederlandse markt, zijn er ook use cases waarin vergelijkbare initiatieven in het buitenland worden gevolgd?
Wanneer het voor een use case relevant is worden relevante initiatieven in het buitenland gemonitord, een sectoraal initiatief voor de gebouwde omgeving vergelijkbaar met het DSGO is op het moment niet bekend bij het DSGO-programma.

Hoe zorgt het DSGO-programma dat de implementatielast voor het MKB niet te hoog wordt?
Het DSGO-programma is bewust dat de gebouwde omgeving bestaat uit een groot aantal MKBers voor welke de implementatielast van datadiensten relatief hoog kan zijn. Het DSGO biedt een aantal hulpmiddelen om de implementatielast te verlichten, bijvoorbeeld door gebruik te maken van een data-broker (in de volgende release van het afsprakenstelsel wordt deze nieuwe rol geïntroduceerd). Daarnaast is het van belang dat softwareleveranciers het DSGO in hun systemen gaan ondersteunen zodat partijen die de vereisten in het DSGO niet zelf kunnen implementeren dit kunnen afnemen bij haar softwareleverancier.

Hoe wordt één datadienst binnen het DSGO gedefinieerd?
Een datadienst is een dienst waarin data wordt gedeeld of bewerkt. Een datadienstaanbieder is verantwoordelijk voor het definiëren van één of meer datadiensten en verantwoordelijk om de datadienst in lijn met de definitie aan te bieden. Daarmee bepaalt de datadienstaanbieder o.a. de scope, inhoud, functionaliteit, datamodellen en voorwaarden van de aangeboden datadienst is (zie de pagina Wat is een datadienst?).

Zijn er binnen het DSGO naast decentrale datadiensten ook centrale diensten beschikbaar?
Datadiensten vinden plaats tussen een datadienstaanbieder en datadienstgebruiker. Om dit mogelijk te maken levert het DSGO stelselvoorzieningen en worden in het afsprakenstelsel vereisten gesteld aan marktvoorzieningen. Voorzieningen zijn ondersteunende faciliteiten die nodig zijn voor het functioneren van



digitaal samenwerken in de Gebouwde Omgeving

Samenvatting discussiepunten vervolg

Betreft
Technische werkgroep DSGO

het DSGO. Voorzieningen zijn voor gemeenschappelijk gebruik, en ondersteunen partijen bij de implementatie en bij gebruik van het DSGO. Sommige voorzieningen, bijvoorbeeld de stelselcatalogus, leveren centrale diensten (zie Wat zijn voorzieningen).

Welke certificaten hebben partijen nodig die van het DSGO gebruik willen maken en wat zijn de doeleinden van de verschillende certificaten?
Het DSGO maakt gebruik van twee soorten certificaten voor verschillende doelen. Beide certificaten worden uitgegeven door aanbieders van vertrouwensdiensten onder de eIDAS verordening: Qualified website authentication certificates (QWACs) e**n** Qualified Certificate for Electronic Seals (QSEAL)**.** Zowel QWACs als QSEALs moeten eenmalig worden aangevraagd en kunnen daarna als volgt worden gebruikt (zie ook pagina Informatiebeveiliging):

QWACS:

- Het gebruik van QWACs door datadienstaanbieders is voor het beveiligen van de communicatie en stelt datadienstgebruikers in staat om de identiteit van de datadienstaanbieder vast te stellen
- Het is de verantwoordelijkheid van datadienstaanbieders om een QWAC aan te vragen en te gebruiken voor one-way (server only) TLS (minimaal v1.2)

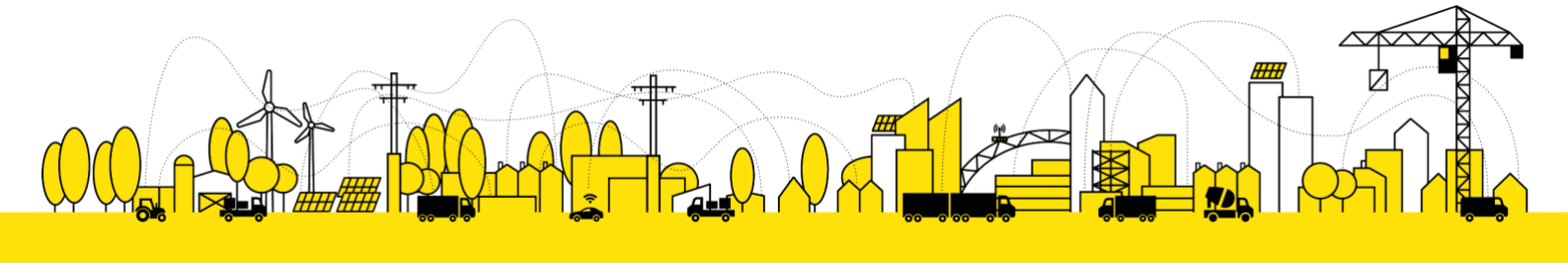
QSEALs:

- Bij zowel het API verzoek en de respons kan gebruik gemaakt worden van JSON Web Tokens, getekend met QSEALs
- JWTs getekend door QSEALs worden gebruikt om de identiteit van de verzender te valideren
- Verder worden JWTs getekend met QSEALS gebruikt om berichten onweerlegbaar te binden aan de verzender

Waarom maakt het DSGO gebruik van twee verschillende mechanisme voor de authenticatie van datadienstgebruiker en datadienstaanbieders?
Authenticatie met QWACs is voor beide de datadienstaanbieder en de datadienstgebruiker mogelijk middels two-way TLS. Echter, dit brengt een zwaardere implementatielast met zich mee voor de datadienstgebruiker, die niet voor elke datadienst nodig is.

Het gebruik van QSEALs kan naast authenticatie worden gebruikt om de onweerlegbaarheid van berichten te borgen. Dit is van belang vanuit juridisch perspectief en draagt bij aan het vertrouwen wat nodig is om data delen in een netwerk mogelijk te maken. Hierom is het gebruik van QSEALs verplicht voor zowel datadienstaanbieders als datadienstgebruikers. Omdat voor deze reden QSEALs gebruikt worden, kunnen deze hergebruikt worden voor authenticatie doeleindes.

De combinatie van vereisten betreft server-side TLS en het tweezijdig gebruikt van QSEALs, maakt het mogelijk om voor veel verschillende datadiensten in het DSGO in voldoende mate authenticiteit en onweerlegbaarheid



Samenvatting discussiepunten vervolg

Betreft
Technische werkgroep DSGO

te kunnen garanderen. Hoewel deze vereisten voor sommige datadiensten overbodig zijn bevorderden de eisen zoals opgesteld in het DSGO de interoperabiliteit tussen verschillende partijen (zie Informatiebeveiliging).

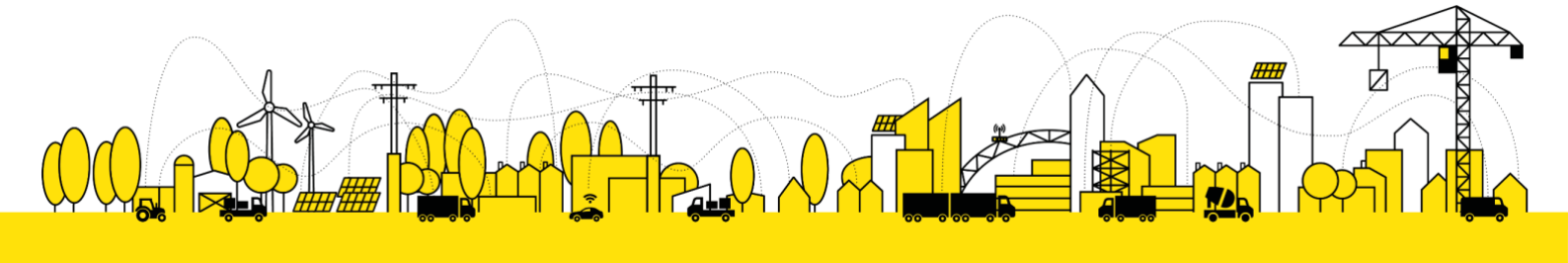
Hoe verhoudt autorisatie bij human-to-machine datadiensten zich tot autorisatie bij machine-to-machine datadiensten?
Voor human-to-machine interacties in de context van datadiensten wordt voorzien dat dit typisch plaatsvindt via een persoon die haar rechten delegeert, waarbij de datadienst machine-to-machine wordt uitgevoerd en de gedelegeerde rechten worden gecontroleerd.

Wat betekent autorisatie binnen het DSGO en wanneer is autorisatie van toepassing?
Autorisatie is het hebben van rechten of toestemming en het proces waarbij een partij rechten of toestemming krijgt om een specifieke actie uit te voeren. Autorisatie is een overkoepelend onderwerp waarbinnen het mogelijk is om rechten te delegeren. Het DSGO definieert drie aspecten van autorisatie, het autorisatiebeleid opstellen, de autorisatie-informatie organiseren, en het autorisatiebesluit nemen. Bij iedere datadienst moet de georganiseerde autorisatie-informatie getoetst worden tegen het autorisatiebeleid om een autorisatiebesluit te nemen, de complexiteit hierin verschilt per datadienst.

Het delegeren van rechten is een mogelijkheid die optioneel is bij het organiseren van de autorisatie-informatie en niet voor iedere datadienst relevant is. Het mogelijk dat gedelegeerde rechten moeten worden opgehaald bij een autorisatieregister. Het is ook mogelijk dat delegatie helemaal geen rol speelt en om te autoriseren bij verschillende instanties gecontroleerd wordt of een datadienstgebruiker over de juiste kwalificaties beschikt om een datadienst af te nemen (zie Autorisatie).

Hoe verhouden de rollen van de rechthebbende en de datadienstaanbieder zich tot elkaar bij het bepalen van de toegangscontroleregels?
De datadienstaanbieder is verantwoordelijk voor het definiëren van toegangscontroleregels voor haar datadienst. Dit bevat wie de rechthebbende is, tot welke (delen van) datadiensten rechthebbende gerechtigd zijn en of het mogelijk is om rechten te delegeren aan derde partijen (zie Autorisatie).

Hoe waarborgt het DSGO dat er geen datadiensten uitgevoerd worden waar data die niet vrijgegeven mag worden toch wordt vrijgegeven doordat het autorisatiebeleid niet op orde is?
De inhoud van een datadienst binnen het DSGO is de verantwoordelijkheid van de datadienstaanbieder. Dit geldt dus ook voor de inhoud van de data die in datadiensten wordt gedeeld (zie Scope van het DSGO). Het is vervolgens ook de verantwoordelijkheid van de datadienstaanbieder om datadiensten juist (in lijn met de datadienstdefinitie en wet- en regelgeving) uit te voeren.



digiGO digitaal samenwerken in de Gebouwde Omgeving

Samenvatting discussiepunten vervolg

Betreft
Technische werkgroep DSGO

Voor de generieke afspraken is een generieke DSGO-conformiteitstest-tool in ontwikkeling, maar het is (voorlopig) niet voorzien dat voor iedere datadienst specifieke test-tooling door het DSGO wordt ontwikkeld waarmee volledige datadiensten getest kunnen worden.

Wordt bij ieder verzoek voor een access token in de stelselcatalogus opgehaald of een datadienstgebruiker deelneemt aan het DSGO?
Bij het uitgeven van een access token moet een datadienstaanbieder valideren of een datadienstgebruiker de voorwaarden van het DSGO kent en daaraan gehouden kan worden. Dit kan op twee manieren, of de datadienstaanbieder en de datadienstgebruiker hebben een bilateraal contract, of de datadienstgebruiker heeft een overeenkomst met de beheerorganisatie. In het tweede geval wordt bij het aanvragen van een access token in de stelselcatalogus opgehaald of de datadienstaanbieder deelneemt aan het DSGO.

Moet de rechthebbende zelf handelen bij het autoriseren van een datadienstgebruiker nadat een datadienstverzoek is verstuurd?
De rechthebbende moet actief handelen wanneer er sprake is van delegaties. De rechthebbende mag binnen de mogelijkheden die de datadienstaanbieder daarvoor biedt bepalen waar zij haar delegaties wil registreren. In het geval de rechthebbende haar delegaties zelf beheert moet de datadienstaanbieder bij ieder datadienstverzoek autorisatie-informatie ophalen bij de rechthebbende. Als de rechthebbende haar delegaties niet zelf beheert (maar bij de datadienstaanbieder of een autorisatieregister) moet de rechthebbende voor de uitvoering van een datadienst haar delegaties actief registreren. Zij is dan niet direct betrokken tijdens de uitvoering van de datadienst (in de volgende release van het afsprakenstelsel wordt dit verder toegelicht).

Voorziet het DSGO een ‘‘poortwachter’’ die overeenkomsten tussen datadiensten beoordeelt en vergelijkbare datadiensten standaardiseert zodat er geen wildgroei aan vergelijkbare datadiensten ontstaat?
De samenhang van datadiensten wordt in het programma gemonitord en waar mogelijk geborgd in specifieke afspraken.

Hoe worden binnen het DSGO slimme objecten die data delen geauthentiseerd en/of geautoriseerd?
Slimme objecten worden binnen het DSGO niet geauthentiseerd en/of geautoriseerd. De juridische entiteiten die eigenaar zijn van slimme objecten zijn verantwoordelijk voor het aanbieden en afnemen van datadiensten en daarmee ook om te voldoen aan de vereisten die daarbij komen kijken (zie Identificatie).