# Afsprakenstelsel DSGO

Dit document bevat een volledig overzicht van de huidige status van het Afsprakenstelsel DSGO.


Voor opmerkingen over het afsprakenstelsel DSGO, plaats je opmerking in deze excel sheet en stuur deze naar afsprakenstelseldsgo@digigo.nu voor 9 november. Opmerkingen zijn input voor de publieke review:

- op 16 november voor publieke review functioneel en juridisch (klik hier om aan te melden - Dday dag 2)
- op 29 november voor publieke review: technisch (klik hier om je aan te melden)

Ook kan je meepraten in de werkgroep functionele beheerprocessen op 29 november.

## Introductie

- In de Introductie vind je meer informatie over DigiGO, DSGO, en de aanleiding, het doel, scope en Richtinggevende Principes van het Afsprakenstelsel DSGO.
- In Versiebeheer, vind je een overzicht van alle voorgaande en geplande releases.
- In Kern van het Afsprakenstelsel DSGO worden de relevantste thema en onderwerpen waar het afsprakenstelsel aan bijdraagt beschreven.
- De afspraken die van toepassing zijn op alle mogelijke data deel oplossingen in de gebouwde omgeving, zijn te vinden onder Generieke afspraken.
- Sommige oplossingen vereisen specifieke afspraken boven op de generieke afspraken om te worden mogelijk gemaakt. Deze staan beschreven in de Specifieke afspraken.
- In de Appendix staan o.a. de begrippenlijst, FAQ, en bronnen.

Het afsprakenstelsel bevat conceptafspraken die onderdeel van het DSGO zullen gaan vormen.

**Merk op,** deze conceptafspraken zijn een eerste voorzet ter discussie. Ze zijn voor een deel gebaseerd op best practices, maar leggen hier en daar ook een ambitie neer. Het afsprakenstelsel wordt verder ontwikkeld in nauwe samenwerking met marktpartijen waarin de inhoud wordt behandeld en de afspraken verder aangescherpt en aangevuld. Zie de Aanpak ontwikkeling van het Afsprakenstelsel DSGO voor meer informatie over het proces.

---

## Inhoudsopgave

Search

# Introductie

Deze pagina's bevatten de conceptafspraken die samen het afsprakenstelsel van het DSGO zullen gaan vormen.

> **Merk op,** deze conceptafspraken zijn een eerste voorzet ter discussie. Ze zijn voor een deel gebaseerd op best practices, maar leggen hier en daar ook een ambitie neer. Het afsprakenstelsel wordt verder ontwikkeld in nauwe samenwerking met marktpartijen waarin de inhoud wordt behandeld en de afspraken verder aangescherpt en aangevuld. Zie de Aanpak ontwikkeling afsprakenstelsel DSGO voor meer informatie over het proces.

In dit deel wordt het DSGO-programma en het afsprakenstelsel geïntroduceerd:

# Aanleiding programma Digitaal Stelsel Gebouwde Omgeving

De komende jaren staat de gebouwde omgeving voor een aantal grote maatschappelijke opgaven. Denk daarbij aan de klimaatopgave (verduurzamen woningvoorraad, circulaire-economie, hoogwaterbescherming, hittestress), het oplossen van de woningnood (verdichten, nieuwbouw), de grote onderhouds- en vervangingsoperatie van onze infrastructuur en zeker niet op de laatste plaats de stikstofproblematiek.

Het realiseren van de genoemde opgaven vereist betere samenwerking, nieuwe toepassingen en het daartoe delen van data tussen ketenpartners in de gebouwde omgeving. Om te werken aan de toegankelijkheid van data in de gehele keten is het programma Digitaal Stelsel Gebouwde Omgeving (DSGO) gestart. Zie voor meer informatie over het DSGO-programma de website en het programmaplan.

## Visie van het DSGO-programma

Het DSGO is randvoorwaardelijk voor beter en betrouwbaar data delen in de gebouwde omgeving. Het DSGO biedt een set van uniforme afspraken, die zorgen voor veilige, betrouwbare en gecontroleerde toegang tot data.

Daarmee beoogt het DSGO-programma dat partijen in de gebouwde omgeving makkelijker de juiste data kunnen delen voor verschillende use cases en voldoende vertrouwen en kennis hebben om data delen in te willen zetten. Hierdoor is het mogelijk om bestaande digitaliseringsinitiatieven tussen ketenpartners op te schalen en nieuwe toepassingen mogelijk te maken.

## Doelstelling van het DSGO-programma

De strategische doelstelling van het DSGO-programma is: het makkelijker en betrouwbaarder data delen in de gebouwde omgeving tussen ketenpartners op basis van datadiensten mogelijk gemaakt door het DSGO. Om dit te realiseren werkt het programma aan het ontwerpen, realiseren en in beheer (doen) nemen van het DSGO.

:Quotes:

**Bron:** Programma Plan DSGO - 1.2 Visie en doelstelling DSGO-programma

Het ontwerpen, realiseren en in beheer (doen) nemen van het DSGO, op basis waarvan ketenpartners datadiensten kunnen (laten) ontwikkelen, waarmee eenvoudig op een veilige, betrouwbare en toegankelijke manier gericht data gedeeld en/of bewerkt kan worden.

Het DSGO bestaat uit een set uniforme afspraken, het afsprakenstelsel, en bijbehorende voorzieningen. Het afsprakenstelsel maakt een federatief ecosysteem voor data delen tussen ketenpartners mogelijk. Dit afsprakenstelsel wordt gepresenteerd in deze onlineomgeving.

Naast het DSGO levert het DSGO-programma ook ondersteunende informatie en generieke communicatie over het DSGO.

Gedurende de looptijd van het programma (januari 2022 t/m juni 2024) wordt een eerste operationele versie van het DSGO ontworpen en geïmplementeerd, en overgedragen aan een beheerorganisatie.

# Doel van het Digitaal Stelsel Gebouwde Omgeving

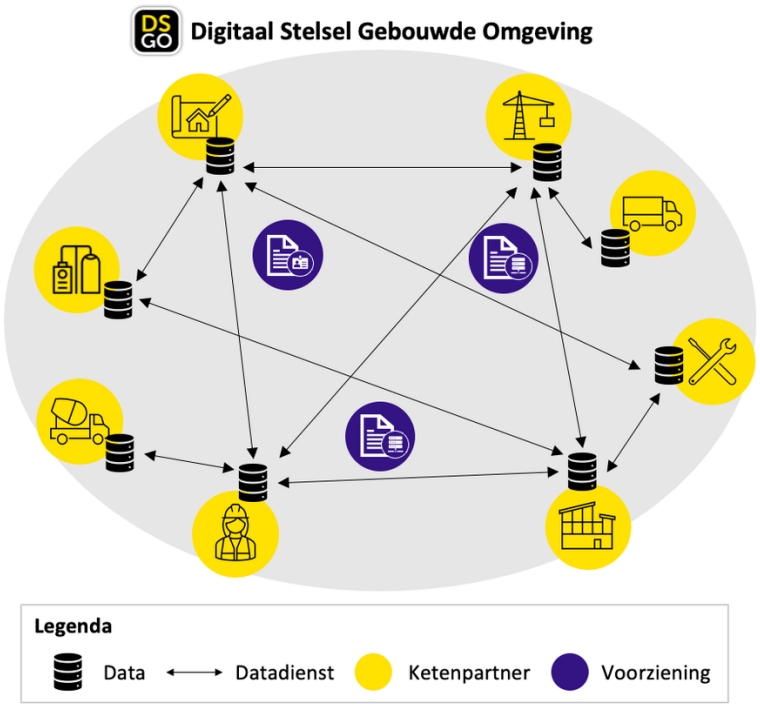
Het doel van het DSGO-programma is het ontwerpen, realiseren en in beheer (doen) nemen van het Digitaal Stelsel Gebouwde Omgeving (DSGO). Het DSGO faciliteert een netwerk van datadiensten om in de gebouwde omgeving data te delen en/of te bewerken in een federatief ecosysteem o.b.v. afspraken en voorzieningen.

- Het afsprakenstelsel DSGO biedt afspraken om op gestandaardiseerde wijze datadiensten te implementeren.
- Voorzieningen bieden ondersteunende faciliteiten die nodig zijn voor het functioneren van het DSGO.

**Merk op,** het DSGO heeft als doel het faciliteren van datadelen in de gebouwde omgeving. Het DSGO is data agnostisch, dus zal alle mogelijke data ondersteunen. Daarmee wordt de term 'data' als overkoepelende term gebruikt voor onder andere ruwe gegevens, informatie en documenten.

## Wat is een federatief ecosysteem voor datadelen?

Een federatief ecosysteem voor datadelen stelt deelnemende partijen in staat om data vanuit de bron beschikbaar te stellen aan andere partijen middels datadiensten. Het federatief ecosysteem van deelnemers vormt samen met gemeenschappelijke voorzieningen een netwerk waarbinnen ketenpartners in staat zijn om (met de juiste autorisatie) data te delen. Hiermee krijgen ketenpartners verantwoord actueel inzicht in data. Deelnemers aan het federatief ecosysteem hebben inspraak in de governance, georganiseerd via de beheerorganisatie van het DSGO.




DSGO levert afspraken en gemeenschappelijke voorzieningen die dienen als fundament voor een netwerk van datadiensten in de gebouwde omgeving

Een federatief ecosysteem voor datadelen kent een aantal belangrijke aspecten:

- **Juiste partijen krijgen toegang tot relevante data:** Datadelen wordt mogelijk met directe relaties, maar ook met relaties van relaties (met de juiste toestemming) waardoor ook over ketens heen data gedeeld wordt.

- **Degene die rechten heeft over data blijft in controle:** Er ontstaat vertrouwen tussen partijen omdat degene die rechten heeft over de data in controle blijft onder welke voorwaarden wie wat met de data mag doen. Daarmee kan data niet zonder toestemming verder worden gedeeld.
- **Geen onnodige data replicatie:** Doordat verschillende partijen toegang krijgen tot (delen van) dezelfde dataset vanuit de bron, hebben partijen de garantie dat ze het over dezelfde data hebben en niet werken met kopieën met versieverschillen ertussen.
- **Inspraak in de governance van het ecosysteem:** Wanneer een partij aan alle eisen voldoet en kiest om deel te nemen aan het DSGO, krijgt de partij inspraak in het beheer en de doorontwikkeling van het federatief ecosysteem.

## Wat is een afsprakenstelsel?

Het afsprakenstelsel DSGO vormt het fundament voor een digitaal federatief ecosysteem in de gebouwde omgeving. Door de gemeenschappelijke afspraken ontstaat een gelijk speelveld waarin deelnemers aan het DSGO veilig, vertrouwd en geautoriseerd data kunnen delen in een federatief ecosysteem.

:Quotes:

**Bron:** Logius - Wat is een Afsprakenstelsel?

Afsprakenstelsels, of kortweg ‘stelsels’, zijn nauwe samenwerkingsvormen van verschillende partijen uit het bedrijfsleven, de overheid en de wetenschap, die producten of diensten leveren, op basis van vastgelegde eisen. Bijvoorbeeld aan een identiteitssysteem of een online betaalsysteem. In het Engels wordt een afsprakenstelsel *Trust Framework* genoemd.

Op basis van deze definitie is het afsprakenstelsel DSGO gedefinieerd als: **“**een set afspraken tussen deelnemers aan het DSGO en is daarmee het fundament voor harmonisatie en vertrouwen om een federatief ecosysteem voor datadelen te realiseren.”

De scope van het afsprakenstelsel DSGO wordt verder gedetailleerd op de onderliggende pagina. Verder vormt het BLOFT-raamwerk (geformuleerd door de Data Sharing Coalition in het Data Sharing Canvas) het startpunt voor het maken van afspraken die binnen het afsprakenstelsel opgenomen worden. Het BLOFT-raamwerk bevat een breed scala aan onderwerpen waarover afspraken nodig zijn voor het creëren van vertrouwen en harmonisatie binnen een ecosysteem.

## Wat zijn voorzieningen?

Voorzieningen zijn ondersteunende faciliteiten die nodig zijn voor het functioneren van het DSGO. Voorzieningen zijn voor gemeenschappelijk gebruik, en ondersteunen partijen bij het uitvoeren van datadiensten en in de voorbereiding daarop.

De minimale vereisten aan alle voorzieningen worden gedefinieerd gedurende de ontwikkeling van het DSGO. Alle voorzieningen staan onder toezicht van de beheerorganisatie DSGO. Voorzieningen die door de beheerorganisatie DSGO worden geleverd heten stelselvoorzieningen, en voorzieningen die door partijen in de gebouwde omgeving worden geleverd heten marktvoorzieningen. Op dit moment worden de volgende voorzieningen voorzien als onderdeel van het DSGO, zie het figuur hieronder.


Overzicht van de verschillende type voorzieningen en wanneer ze gebruikt worden

Merk op, deze lijst kan in verloop van tijd aangevuld en/of aangepast worden.

### Stelselvoorzieningen

- Developer portal: Een online interface waar ontwikkelaars documentatie tools en middelen kunnen vinden om effectief gebruik te maken van de DSGO specificaties, waardoor ze gemakkelijk softwaretoepassingen kunnen bouwen en integreren
- Conformiteitstest-tool: een software hulpmiddel dat is ontworpen om de beheerorganisatie DSGO te laten verifiëren of de implementatie van een API voldoet aan het afsprakenstelsel
- Stelselcatalogus: een overzicht van deelnemers en datadiensten in het DSGO om andere partijen de benodigde informatie te bieden voor het vinden en uitvoeren van datadiensten.

### Marktvoorzieningen

- Authenticatiediensten, autorisatieregisters en datadienstbrokers: Optionele diensten voor gemeenschappelijk gebruik in het DSGO ondersteunen waar relevant en nodig. De noodzaak van het gebruik van marktvoorzieningen in een datadienst is afhankelijk van de specifiek use case / toepassing van de datadienst.

Op dit moment volgt het DSGO het iSHARE afsprakenstelsel voor alle eisen van authenticatiediensten en autorisatie registers. Voor meer informatie over authenticatiediensten (Identity providers) en autorisatieregisters (Authorization registry) zie iSHARE.

# Scope van het Digitaal Stelsel Gebouwde Omgeving

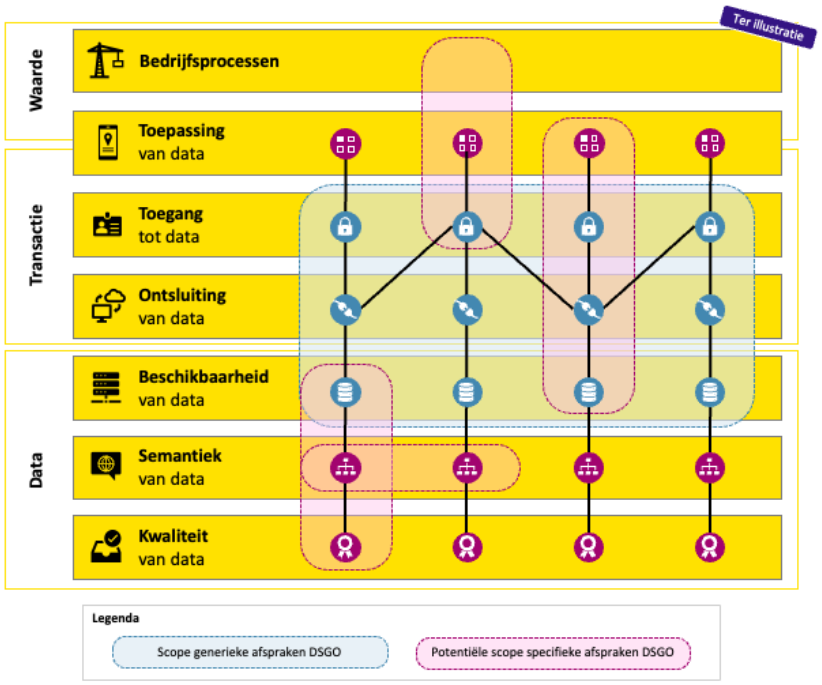
In de gebouwde omgeving wordt in ketens waarde gecreëerd door en voor diverse partijen. Daartoe voeren (keten)partijen activiteiten uit in bedrijfsprocessen (zowel intern als tussen ketenpartijen), gebruikmakend van bedrijfsspecifieke applicaties. Om het doel van de applicaties te bereiken wordt in deze applicaties data toegepast. Mogelijk wordt de toegepaste data weer beschikbaar gesteld voor andere toepassingen. Onderliggend aan deze bedrijfsprocessen (applicaties) vinden transacties plaats waarbij data wordt gedeeld naar applicaties.

⭐ Voorbeelden van waardecreatie in de gebouwde omgeving op basis van bedrijfsprocessen, transacties en gebruikte data:

- Tussen partijen zoals opdrachtgever en architect vindt een ‘opdrachtverstrekking’ transactie plaats waarbij (onder ander) een offerte en een opdracht bevestiging wordt gedeeld.
- Tussen partijen zoals ontwikkelaar en woningbouwcorporatie vindt het ‘opleveren van een woning’ plaats waarbij (onder andere) een bouwwerk dossier wordt gedeeld.
- Tussen partijen zoals opdrachtgever en aannemer vindt een 'planningsdata' transactie plaats waarbij (onder andere) de actuele leveringstijden wordt gedeeld.

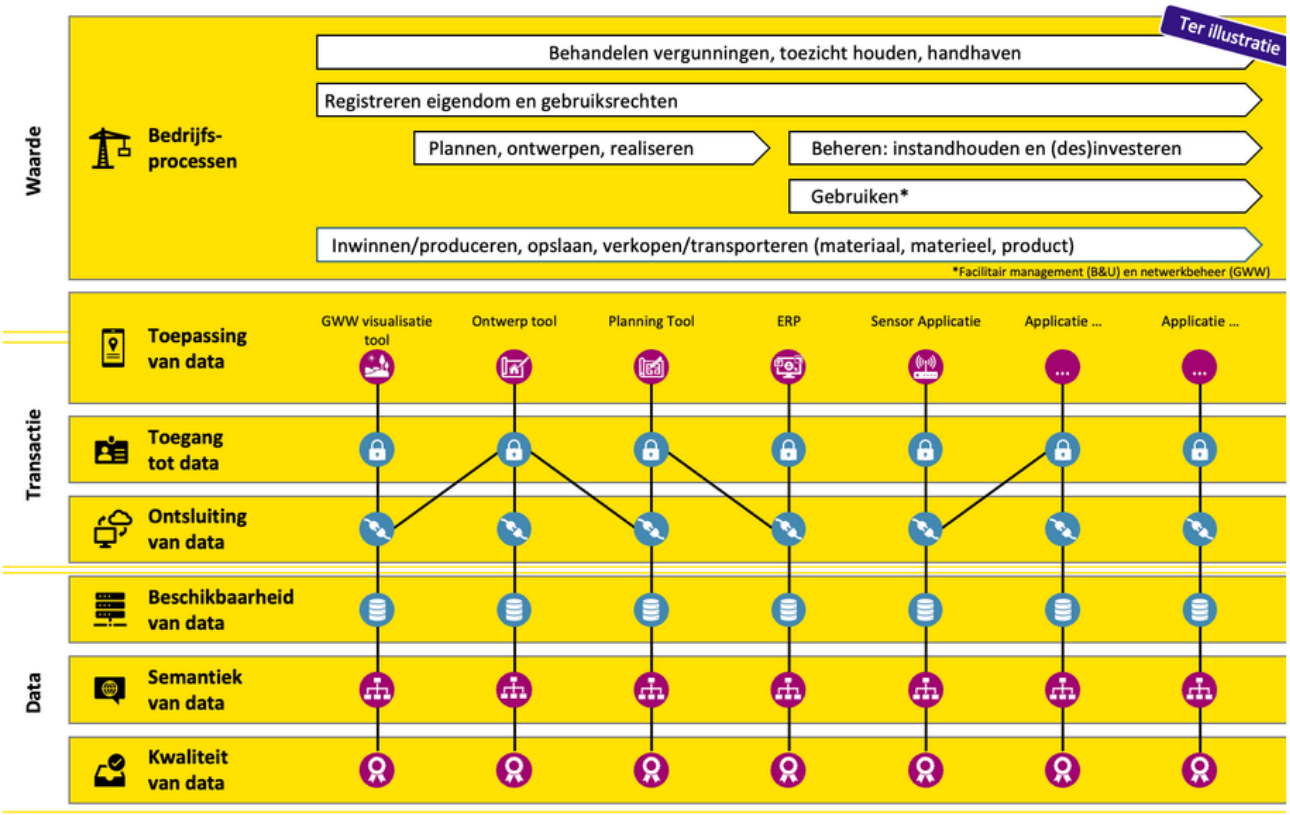
Via het DSGO wordt gezorgd voor makkelijkere, toegang, ontsluiting en beschikbaarheid van en tot data die nodig is bij het voeren van bedrijfsprocessen. Het afsprakenstelsel bestaat uit generieke afspraken en specifieke afspraken. Generieke afspraken gelden voor (de ondersteuning van) alle mogelijke datadiensten, en zijn daarmee data agnostisch (niet afhankelijk van de data die wordt gedeeld). Hiermee zijn bedrijfsprocessen, de toepassingen, de semantiek en de kwaliteit van data buiten scope van de generieke afspraken van het afsprakenstelsel.

Naast generieke afspraken kunnen specifieke afspraken worden gemaakt op basis van concrete toepassingen uit de praktijk (zie de aanpak ontwikkeling afsprakenstelsel DSGO). Specifieke afspraken gelden voor specifieke data, zijn daarmee niet data agnostisch en relevant voor enkele delen van de gebouwde omgeving. Specifieke afspraken kunnen een bredere scope hebben dan generieke afspraken, en kunnen bijvoorbeeld afspraken bevatten over bedrijfsprocessen, de toepassingen, de semantiek en de kwaliteit van data die gedeeld wordt.



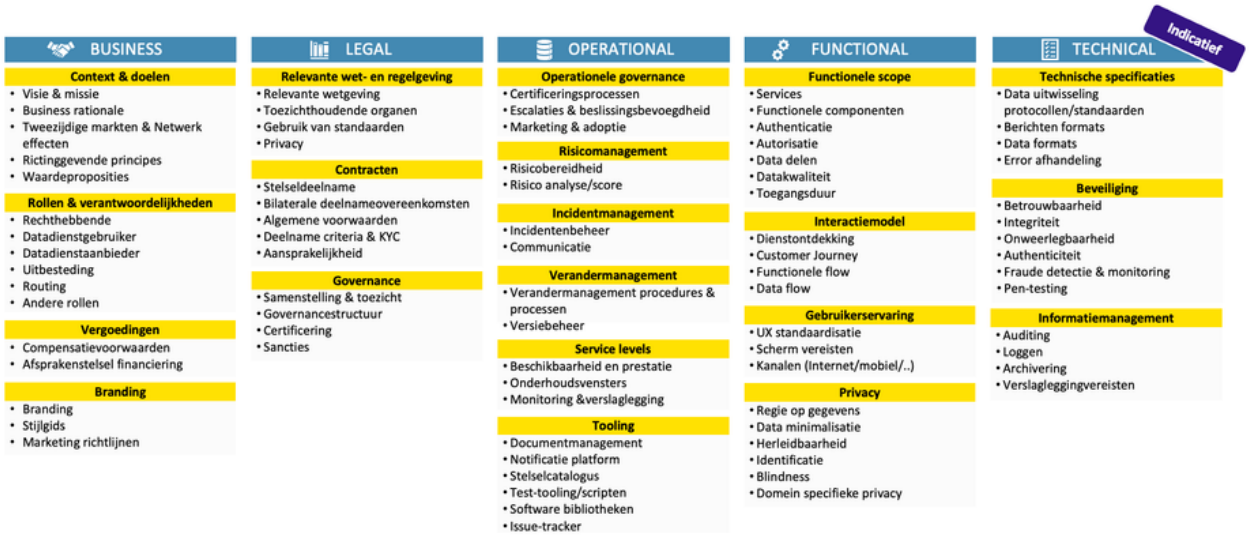

Het afsprakenstelsel legt generieke afspraken en specifieke afspraken vast als fundament voor het delen van data voor toepassingen in bedrijfsprocessen

In het onderstaande voorbeeld worden enkele voorbeeld bedrijfsapplicaties getoond die gebruikt worden in verschillende bedrijfsprocessen.


Ter illustratie
Waarde
Bedrijfs-processen
Behandelen vergunningen, toezicht houden, handhaven
Registreren eigendom en gebruiksrechten
Plannen, ontwerpen, realiseren
Beheren: instandhouden en (des)investeren
Gebruiken*
Inwinnen/produceren, opslaan, verkopen/transporteren (materiaal, materieel, product)
*Facilitair management (B&U) en netwerkbeheer (GWW)
Transactie
Toepassing van data
GWW visualisatie tool
Ontwerp tool
Planning Tool
ERP
Sensor Applicatie
Applicatie ...
Applicatie ...
Toegang tot data
Ontsluiting van data
Data
Beschikbaarheid van data
Semantiek van data
Kwaliteit van data

# Het BLOFT-raamwerk

Het BLOFT-raamwerk is door de Data Sharing Coalition geformuleerd in het Data Sharing Canvas op basis van ervaringen van het maken van afsprakenstelsels in het verleden. Het bevat een uitgebreide lijst van onderwerpen die samen een startpunt vormen voor het maken van een blauwdruk voor een afsprakenstelsel voor data delen.




Op het eerste gezicht geeft dit model een uitgebreid overzicht. In de praktijk is de scheiding van onderwerpen niet zo duidelijk als aangegeven, omdat er overlap is tussen onderwerpen en onderwerpen vanuit verschillende perspectieven kunnen worden besproken. Daarom wordt dit uitgebreide BLOFT-raamwerk gebruikt als startpunt om ervoor te zorgen dat alle onderwerpen aan bod komen tijdens de ontwikkeling van het afsprakenstelsel.

Merk op dat veel bestaande standaarden/richtlijnen/normen reeds gebruikte technische specificaties hebben. In het afsprakenstelsel zal de relatie met, en het gebruik van bestaande technische standaarden gedetailleerd worden.

# Illustratieve voorbeelden van het DSGO

Twee verhalen zijn uitgewerkt als praktisch voorbeeld van use cases die mogelijk zijn met het (toekomstige) DSGO. Deze verhalen zijn alleen ter illustratie om een gevoel te geven van de waarde die gerealiseerd kan worden met het DSGO.

1. Delen van productdata als voorbeeld case
2. Delen van planningsdata in een bouwhub als voorbeeld case

**Merk op,** het DSGO draagt bij aan het aanbieden van vele verschillende datadiensten en daarmee use cases. Datadiensten vinden plaats tussen DSGO gebruikers. De bovenstaande voorbeelden illustreren hoe één datadienst kan werken in de samenwerking tussen twee ketenpartners.

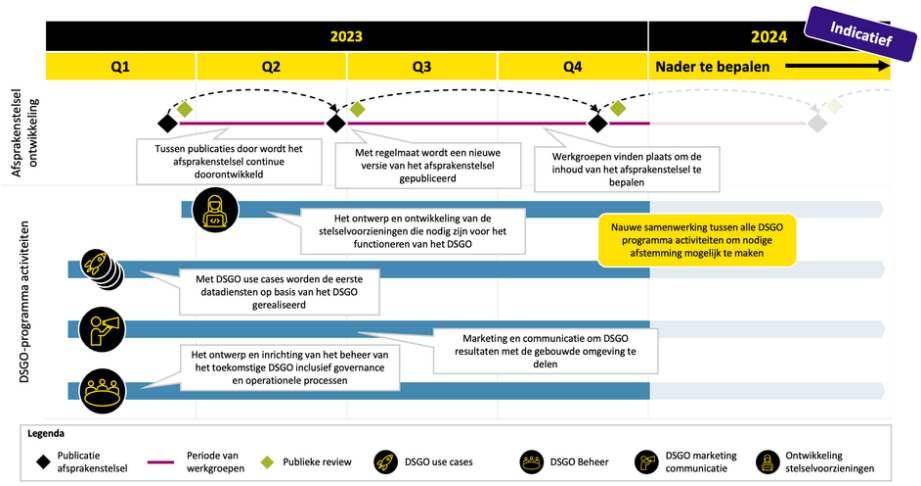
# Aanpak ontwikkeling van het Afsprakenstelsel DSGO

Voor opmerkingen over het afsprakenstelsel DSGO, plaats je opmerking in deze excel sheet en stuur deze naar afsprakenstelseldsgo@digigo.nu voor 9 november. Opmerkingen zijn input voor de publieke review:

- op 16 november voor publieke review functioneel en juridisch (klik hier om aan te melden voor de Dday dag 2)
- op 29 november voor publieke review: technisch (klik hier om je aan te melden)

Ook kan je meepraten in de werkgroep functionele beheerprocessen op 29 november.

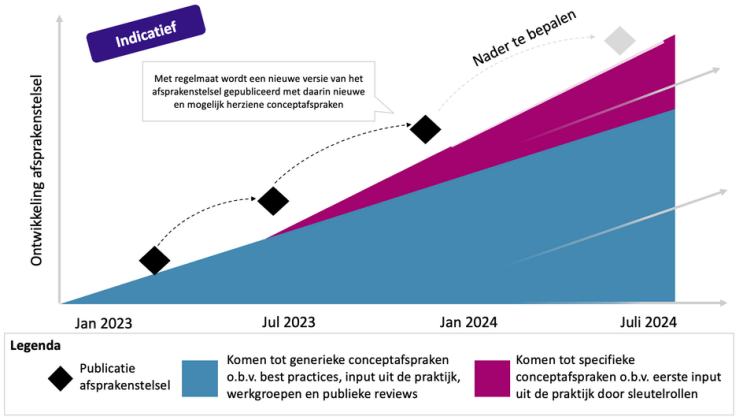
Het Afsprakenstelsel DSGO wordt ontwikkeld als onderdeel van het DSGO-programma. Voor meer informatie, zie de digiGO website. In de ontwikkeling van het afsprakenstelsel wordt nauw samengewerkt met andere DSGO-programma activiteiten. In de figuur hieronder worden de aanpak voor de ontwikkeling van het afsprakenstelsel gepresenteerd, samen met de belangrijkste DSGO-programma activiteiten weergegeven, inclusief het ontwerpen en ontwikkelen van voorzieningen, datadiensten realiseren met use cases, communicatie en educatie, en ontwerp en inrichting van de toekomstige beheerorganisatie.




Aanpak ontwikkeling van het afsprakenstelsel DSGO hangt nauw samen met andere DSGO-programma activiteiten

Tussen publicaties van het afsprakenstelsel wordt het afsprakenstelsel voortgebracht door middel van werkgroepen, publieke reviews en inzichten uit andere activiteiten wanneer relevant. In iteraties worden nieuwe versies van het afsprakenstelsel gepubliceerd. Het afsprakenstelsel bestaat uit generieke en specifieke afspraken, zie scope van het DSGO. Het DSGO-programma gaat aankomende periode samen met partijen uit de gebouwde omgeving afspraken ontwikkelen in werkgroepen, en toetsen in publieke reviews.

Gedurende het DSGO-programma wordt het afsprakenstelsel ontwikkeld middels een flexibele aanpak. Dit houdt in dat het nog niet mogelijk is om aan te geven welk onderwerp in welke iteratie van het afsprakenstelsel gepubliceerd zal worden. Dit is afhankelijk van wat (er door de sector) geagendeerd wordt in werkgroepen, publieke reviews en inzichten uit use cases van DSGO use cases. Het BLOFT-raamwerk (geformuleerd door de Data Sharing Coalition in het Data Sharing Canvas) geeft een overzicht van de relevante onderwerpen die voorzien worden als generiek en specifieke afspraken in het afsprakenstelsel.

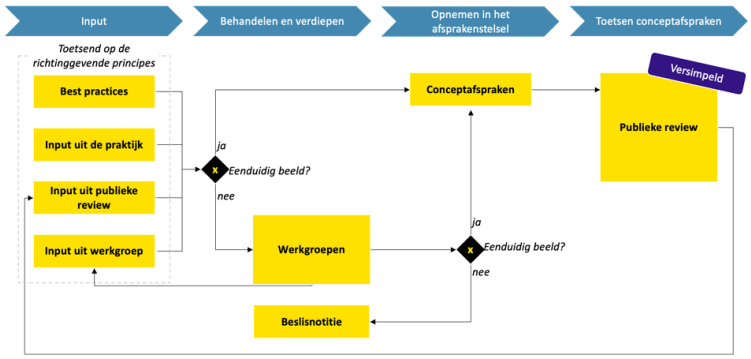



Het afsprakenstelsel wordt iteratief ontwikkeld

## Komen tot conceptafspraken

Om tot een overeenstemming te komen over de inhoud van afspraken in het afsprakenstelsel, wordt een standaard proces gefaciliteerd door het projectteam Afsprakenstelsel, zoals geschetst in de onderstaande figuur. Dit standaard proces geldt voor afspraken binnen de scope van het DSGO (zie scope van het DSGO): Input voor mogelijke afspraken wordt geleverd op basis van best practices, voorbeelden vanuit de praktijk, werkgroepen en de resultaten van publieke review. Alle input wordt getoetst tegen de scope en de richtinggevende principes van het DSGO. De input wordt vervolgens gestructureerd in onderwerpen die ter discussie kunnen worden gesteld in werkgroepen.

Voor alle onderwerpen, zowel die mogelijk generieke als specifieke afspraken betreffen, is het noodzakelijk dat de juiste stakeholders en experts uit de sector betrokken zijn. De resultaten van de werkgroepen worden opgenomen in het afsprakenstelsel als conceptafspraken en worden behandeld in de volgende iteratie van een publieke review. Op deze wijze kan de hele sector via de publieke review input leveren op de conceptafspraken. Indien de publieke review daarvoor aanleiding geeft, kan een conceptafspraak opnieuw als input worden ingediend (nadat het publieke review commentaar is verwerkt).




Middels werkgroepen wordt eenduidig beeld over de input bepaald en worden deze als conceptafspraak opgenomen in het afsprakenstelsel

## Input vanuit de praktijk

In de gebouwde omgeving zijn er samenwerkingsverbanden waar partijen actief samen werken om data deel implementaties te realiseren op basis van het DSGO. Dit kan onder begeleiding van het DSGO als een DSGO use case, of vanuit bestaande initiatieven in de sector. Binnen een samenwerkingsverband kunnen afspraken worden gemaakt over gebruik van standaarden, processen of andere elementen die relevant zijn voor data delen binnen die context. Indien betrokken partijen van mening zijn dat deze afspraken de hele sector ten goede zouden komen en zij sleutelrollen vervullen in de data deel implementatie, dan kunnen deze worden ingediend als input voor het afsprakenstelsel (middels een e-mail naar afsprakenstelseldsgo@digigo.nu). Dit kan leiden tot concept generieke afspraken of tot concept specifieke afspraken.

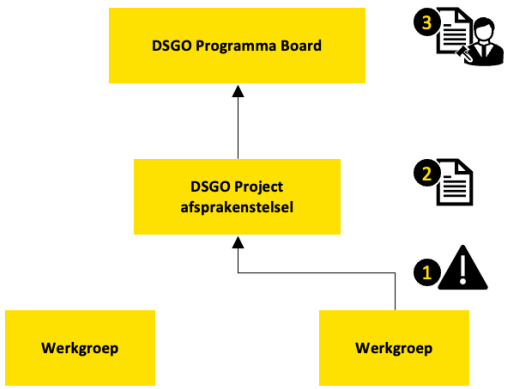
**Merk op,** eerste input voor specifieke afspraken dient te allen tijde te komen uit voorbeelden uit de praktijk door partijen die sleutelrollen in het DSGO (zullen) vervullen. Hiermee wordt geborgd dat specifieke afspraken daadwerkelijk ondersteund worden door haar gebruikers en voorkomt een product push.

Input vanuit de praktijk wordt vervolgens meegenomen in het proces voor komen tot afspraken zoals geschetst hierboven. De input wordt door het projectteam Afsprakenstelsel getoetst tegen de scope van het DSGO en de richtinggevende principes om te controleren of het in aanmerking komt voor een generiek of specifieke afspraak in het afsprakenstelsel. Indien hier een conceptafspraak uit voortvloeit, wordt deze opgenomen in het afsprakenstelsel in afstemming met de indienende partijen.

## Escalatieproces

Als er in een werkgroep punten zijn waar partijen niet met elkaar uit komen, en geen eenduidig beeld ontstaat, dan wordt het escalatieproces gestart wat leidt tot een beslisnotitie, zie onderstaande figuur.

**Let op,** het doel van de werkgroepen is om het escalatieproces zoveel mogelijk te vermijden.




Escalatieproces

1. Als er in een werkgroep punten zijn waar partijen niet met elkaar uit komen, en geen eenduidig beeld ontstaat, dan wordt het escalatieproces gestart.
2. Het DSGO afsprakenstelsel projectteam schrijft een beslisnotitie met daarin:
   - Keuzeopties
   - Afwegingen per optie
   - Reden waarom de keuze niet gemaakt kon worden
   - Gevraagde beslissing DSGO Programma Board
3. Het DSGO Programma Board ontvangt de beslisnotitie en neemt een besluit. Dit wordt teruggekoppeld naar de deelnemers van de werkgroep en wordt opgenomen in het afsprakenstelsel.

# Richtinggevende principes

Bij het maken van het afsprakenstelsel moeten keuzes worden gemaakt over de inhoud van de afspraken. Om het besluitvormingsproces te ondersteunen, wordt gewerkt met een set vooraf opgestelde richtinggevende principes.

Om juist het besluitvormingsproces van het afsprakenstelsel te ondersteunen, zijn de volgende negen richtinggevende principes opgesteld (in willekeurige volgorde):

- Principe 1: Vertrouwd
- Principe 2: Breed toepasbaar
- Principe 3: Toekomstbestendig
- Principe 4: Inclusief
- Principe 5: Kostenefficiënt
- Principe 6: Gebaseerd op open standaarden
- Principe 7: Schaalbaar
- Principe 8: Doelmatig
- Principe 9: Soeverein

## Toepasbaarheid

De richtinggevende principes zijn geen scopebepalingen. De richtinggevende principes geven richting bij het maken van keuzes over de inhoud van het afsprakenstelsel. Tijdens het maken van afspraken binnen het afsprakenstelsel worden er keuzes gemaakt tussen verschillende mogelijke invullingen. Het afwegen van deze keuzes kan lastig zijn omdat het complexe materie betreft, waarbij veel keuzes zowel voor- als nadelen kennen. Daarnaast speelt mee dat bij de ontwikkeling van een afsprakenstelsel een diverse groep van partijen betrokken is, met ieder hun eigen belangen en behoeften. In aanvulling op het inhoudelijke doel en de functionele scope van het afsprakenstelsel, benadrukken de principes een aantal zaken die belangrijk zijn voor het succes van het uiteindelijke afsprakenstelsel. Daardoor kunnen ze steeds worden gebruikt als houvast bij het maken van keuzes tussen verschillende opties voor oplossingen of afspraken.

Deze principes overlappen op sommige onderdelen. Dit betekent dat er meerdere principes van toepassing kunnen zijn op één keuze.

## Principes geven ruimte om te experimenteren

De principes zijn op een zodanig abstractieniveau geformuleerd dat ze richting geven en ondertussen voldoende ruimte bieden om verschillende keuzes te maken. Zo fungeren de principes niet als harde eisen, randvoorwaarden of kader, maar meer als kompas. Hiermee wordt de ruimte voor het verkennen van en experimenteren met verschillende opties en uitwerkingen gemaximaliseerd.

# Principe 1: Vertrouwd

Het afsprakenstelsel dient zodanig ontworpen en onderhouden te worden dat er vertrouwen ontstaat in het stelsel en tussen partijen binnen het stelsel.

## Rationale

Vertrouwen is van essentieel belang voor de waarde van het afsprakenstelsel. Een primaire functie van het afsprakenstelsel is het vergroten van vertrouwen tussen deelnemers onderling, waardoor de waarde van data delen makkelijker kan worden gerealiseerd. Daarnaast is het van belang dat deelnemers voldoende vertrouwen hebben in het afsprakenstelsel zelf.

# Principe 2: Breed toepasbaar

Het afsprakenstelsel als geheel dient als generieke bouwsteen om data delen in een federatief ecosysteem mogelijk te maken in zoveel mogelijk verschillende contexten en toepassingen binnen de gebouwde omgeving. Waar mogelijk dient het afsprakenstelsel interoperabel te zijn met aanpalende sectoren, bijvoorbeeld de energie of logistieke sector.

## Rationale

Door de ontwikkeling van het afsprakenstelsel te richten op de generieke componenten van federatieve data-uitwisseling, kunnen zoveel mogelijk organisaties gebruikmaken van de afspraken die zijn vastgelegd in het afsprakenstelsel. Hierdoor wordt de totale bijdrage van het afsprakenstelsel aan het wegnemen van obstakels voor het delen van data gemaximaliseerd.

# Principe 3: Toekomstbestendig

Het afsprakenstelsel dient toekomstbestendig te zijn door ruimte te bieden voor aanpassingen en uitbreidingen.

## Rationale

De behoeften met betrekking tot het afsprakenstelsel kunnen in de loop der tijd veranderen. Bijvoorbeeld door veranderingen binnen de sector op het gebied van technologie en regelgeving, maar ook door veranderende wensen van de deelnemers. Het afsprakenstelsel moet daarom zijn aan te passen aan deze veranderingen om relevant te blijven.

# Principe 4: Inclusief

Het afsprakenstelsel dient toegankelijk te zijn voor, en te gebruiken te zijn door zoveel mogelijk partijen.

## Rationale

Om de potentiële waarde van data delen te verzilveren is het van belang dat zoveel mogelijk partijen deelnemen aan het stelsel. Hierdoor komt er op grotere schaal data beschikbaar en zijn er meer partijen die gebruik kunnen maken van de beschikbare data. Om dit te bereiken moet het afsprakenstelsel open staan voor nieuwe deelnemers en moeten partijen op een gelijkwaardige manier worden behandeld, zonder dat of onnodig strenge eisen worden opgelegd. Ook partijen die niet direct aan tafel zitten, zoals burgers, kunnen belang hebben bij het afsprakenstelsel. Bij het maken van afspraken dient dan ook met de deze partijen rekening gehouden te worden.

# Principe 5: Kostenefficiënt

Het afsprakenstelsel dient kostenefficiënt te zijn. Het gaat daarbij om de kostenefficiëntie van het gebruik en het beheer van het afsprakenstelsel.

## Rationale

Het beheersen van de kosten is essentieel omdat het direct verband houdt met de waarde die wordt gerealiseerd binnen het afsprakenstelsel. Daarnaast verlaagt het de drempel om te participeren en waarborgt het de duurzame participatie op de lange termijn doordat het de (financiële) lasten van deelname minimaliseert.

# Principe 6: Gebaseerd op open standaarden

Bij de ontwikkeling van het afsprakenstelsel wordt, waar mogelijk en passend, gebruik gemaakt van (delen van) bestaande (open) standaarden, normen en afsprakenstelsels die relevant zijn voor de deelnemende partijen.

## Rationale

Door gebruik te maken van open en bestaande standaarden, normen en afsprakenstelsels wordt maximaal hergebruikt wat er al is en wordt de drempel om deel te nemen aan het afsprakenstelsel verlaagd door de implementatie voor participanten te vergemakkelijken. Daarbij is het van belang dat er voldoende draagvlak is voor de betreffende standaard. Deelnemers zijn minder tijd kwijt aan implementatie en hoeven zo min mogelijk aan te passen in hun bestaande manier van werken.

# Principe 7: Schaalbaar

Het afsprakenstelsel dient berekend te zijn op een groeiend aantal deelnemers en gebruikers.

## Rationale

De gebouwde omgeving bestaat uit een groot aantal partijen dat gebruik moeten kunnen maken van het afsprakenstelsel, het stelsel moet daarom voorbereid zijn op een sterke uitbreiding van het aantal deelnemers, gebruikers en bijbehorend aantal transacties. Door te anticiperen op een groeiend aantal deelnemers en gebruikers, wordt de potentiële waarde van het afsprakenstelsel gemaximaliseerd.

# Principe 8: Doelmatig

Het afsprakenstelsel bevat zoveel afspraken als *nodig* en zo weinig afspraken als *mogelijk* om de doelstellingen te behalen.

## Rationale

Het afsprakenstelsel is erop gericht om het delen van data te vergemakkelijken. Iedere eis of afspraak die niet noodzakelijk is werkt contraproductief, omdat hieraan voldoen leidt tot extra complexiteit voor de (potentiële) deelnemers, zonder dat dat voordeel oplevert. Om deelnemers aan het afsprakenstelsel niet te belasten met onnodige eisen is het van belang het afsprakenstelsel zo beperkt mogelijk te houden.

# Principe 9: Soeverein

De rechthebbende op de data dient altijd de controle te behouden en te bepalen of de data voor een bepaald doel gebruikt mag worden.

## Rationale

Het afsprakenstelsel is erop gericht om het delen van data te vergemakkelijken, maar niet om op te leggen wie welke data zou moeten delen. Soevereiniteit betekent het recht hebben om te beschikken over iets zonder verantwoording aan een ander te hoeven afleggen. Dit vindt altijd plaats binnen de grenzen van wettelijke verplichtingen om bepaalde data uit de wisselen.

# Beheer

Tijdens de looptijd van het DSGO-programma wordt het afsprakenstelsel beheerd door het projectteam Afsprakenstelsel. Neem bij vragen of opmerkingen contact op met afsprakenstelsel@digigo.nu of een van de projectteam leden.



Bauke Rietveld
bauke.rietveld@digigo.nu


Vincent Jansen
vincent.jansen@digigo.nu


Denise Hoppenbrouwer
denise.hoppenbrouwer@digigo.


Tim van Diepenbeek
tim.vandiepenbeek@digigo.nu


Constantijn Molengraaf
constantijn.molengraaf@digigo.


Friso Bergmans
friso.bergmans@digigo.nu


---

Na het DSGO-programma, wordt het beheer van het DSGO uitgevoerd door de beheerorganisatie DSGO die verantwoordelijk is voor doorontwikkeling, adoptie & beheer van het DSGO. De invulling van de toekomstige beheerorganisatie is verder toegelicht op de Governance pagina.

# Leeswijzer (reading guide)

In dit deel wordt de leeswijzer van het afsprakenstelsel beschreven:

- Eisen notatieconventies (requirements notational conventions)
- Typografie (typography)
- Taal (language)

# Eisen notatieconventies (requirements notational conventions)

Het afsprakenstelsel maakt gebruikt van sleutelwoorden om het niveau van eisen aan te duiden, in overeenstemming met IETF RFC 2119 en IETF RFC 8174. Het afsprakenstelsel volgt de Nederlandse interpretatie van deze specificatie zoals vastgelegd door Stichting CROW. De woorden “MOET”, “MAG NIET”, “ZOU MOETEN”, “ZOU NIET MOETEN”, en “MAG” in dit document moeten worden geïnterpreteerd gelijk aan hun Engelstalige equivalenten (“MUST", "MUST NOT / SHALL NOT", "SHOULD", "SHOULD NOT" en "MAY") als beschreven in RFC 2119. Waar deze exacte termen bedoeld zijn worden ze in hoofdletters weergeven. Wanneer deze woorden niet in hoofdletters worden gebruikt, hebben zij hun normale betekenis. De betekenis van deze sleutelwoorden is:

| **Sleutel woord** | **Beschrijving (NL)** | **Key word (EN)** | **Description (EN)** |
|---|---|---|---|
| MOET | alsook "VEREIST" beschrijven een absolute vereiste van de specificatie. | MUST | This word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the specification |
| MAG NIET | en "VERBODEN" beschrijven een absoluut verbod van de specificatie. | MUST NOT | This phrase, or the phrase "SHALL NOT", mean that the definition is an absolute prohibition of the specification. |
| ZOU MOETEN | en "AANBEVOLEN" geven een sterke wens aan, tenzij er een valide reden is om in een specifiek geval af te wijken. De volledige implicaties daarvan MOETEN zorgvuldig gewogen zijn voordat er afgeweken wordt. | SHOULD | This word, or the adjective "RECOMMENDED", mean that there can be valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course. |
| ZOU NIET MOETEN | en "NIET AANBEVOLEN" geven een ongewenste omstandigheid, waarvan volledige implicaties daarvan zorgvuldig gewogen MOETEN zijn voordat het in een specifiek geval toegestaan is. | SHOULD NOT | This phrase, or the phrase "NOT RECOMMENDED", means that there can be valid reasons in particular circumstances when the particular behaviour is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behaviour described with this label. |
| MAG | alsook "MOGEN", "OPTIONEEL" en "NIET VEREIST" geven aan dat dit onderdeel daadwerkelijk optioneel is. De ene aanbieder kan dit onderdeel dan wel implementeren en de ander niet. Een aanbieder die een dergelijke optie niet heeft geïmplementeerd, MOET kunnen omgaan met een aanbieder die dat wel heeft gedaan. En vice-versa. | MAY | This word, or the adjective "OPTIONAL", mean that an item is truly optional. A party may choose to include the item, another party may choose not to. |

Aanwijzing voor het Nederlands: Deze woorden MOGEN verbogen en vervoegd worden. "NIET" kan met "GEEN" vervangen worden, zoals dat gebruikelijk is het Nederlands.

# Typografie (typography)

De typografie in het afsprakenstelsel volgt de volgende regels:

- Gewone tekst verschijnt zo,
- Verwijzingen naar andere bronnen verschijnen zo en bevatten een link naar de bron,

:Quotes: Een grijze achtergrond met aanhalingstekens geeft aan dat de tekst rechtstreeks uit een ander document of een andere bron is geciteerd; op de eerste regel van het grijze kader wordt het document of de bron gespecificeerd,

Een gele achtergrond met groene vink geeft aan dat de tekst een eis/requirement bevat (in lijn met de eisen notatieconventies),

Een blauwe achtergrond met blauwe i geeft aan dat tekst toelichting geeft op het proces of context,

Een paarse achtergrond met gele ster geeft aan dat de tekst een voorbeeld geeft.

# Taal (language)

## Nederlands

Het afsprakenstelsel DSGO is in het algemeen in het nederlands geschreven. Waar relevant, zijn specifieke onderdelen in het Engels, of tweetalig geschreven ten behoeve van (mogelijk) internationale softwareontwikkelaars.

## English

In general, the DSGO trust framework is written in Dutch. Where relevant, specific parts have been written in English, or bilingually for the benefit of (possibly) international software developers.

# Versiebeheer

| Versie | Datum | Beschrijving | Status | Link |
|---|---|---|---|---|
| 0.8 | eind december 2023 | | GEPLAND | |
| | 27 oktober 2023 | Publicatie van het Afsprakenstelsel DSGO ten behoeve van de publieke review op 16 november 2023. Deze onderwerpen zijn toegevoegd in deze publicatie:<br>• Kern van het Afsprakenstelsel DSGO<br>  ◦ Het DSGO rollenmodel<br>  ▪ Rechten en plichten<br>  • Datadienstbroker<br>  ◦ Juridische bepalingen<br>  ◦ Governance<br>• Generieke afspraken<br>  ◦ API specifications<br>  ▪ /capabilities<br>  ▪ /parties<br>  ▪ /trusted_list<br>  ◦ Operationele processen<br>  ▪ Toezicht en handhaving<br>  ▪ Change en releasemanagement<br>  ◦ Autorisatie<br>  ▪ Autorisatie-informatie organiseren<br>  • Delegaties<br>  ◦ Informatiebeveiliging<br>  ▪ Onweerlegbaarheid<br>  ◦ Stelselvoorzieningen<br>• Specifieke Afspraken<br>  ◦ BIM in datadiensten<br>  ▪ BIM voor vergunning of melding afhandelen<br>  • BIM voor vergunning of melding afhandelen voor gebouwen met als gebruiksfunctie woonfunctie<br><br>Deze onderwerpen zijn gewijzigd in deze publicatie:<br>• Kern van het Afsprakenstelsel DSGO<br>  ◦ Het DSGO rollenmodel<br>  ◦ Generiek ondersteunende functionaliteiten<br>  ▪ Abonnement op een gebeurtenis<br>• Generieke afspraken<br>  ◦ Autorisatie<br>  ▪ Autorisatie-informatie organiseren<br>  • Access token | TER REV... | Confluence: Afsprakenstelsel DSGO<br><br>PDF: |

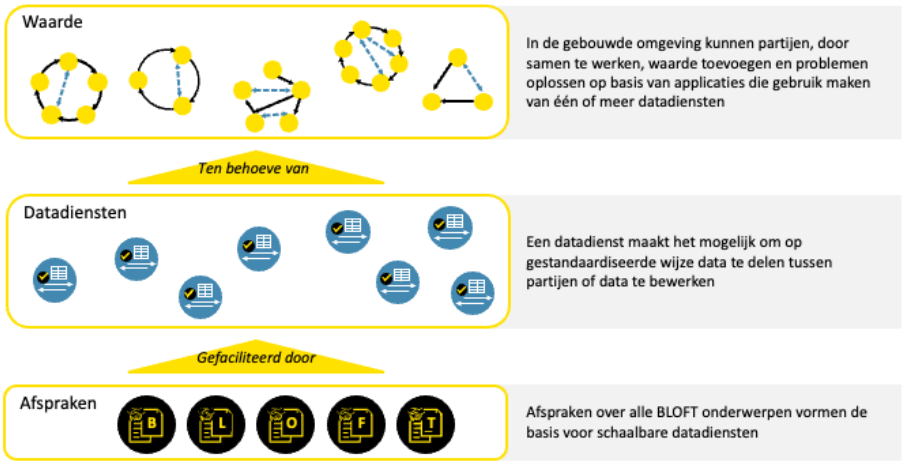
| | | | | |
|---|---|---|---|---|
| | | Deze iteratie op het afsprakenstelsel is gedaan op basis van (onder andere) de input uit de volgende werkgroepen:<br>• Functionele werkgroep, 10 oktober: link verslaglegging<br>• Technische werkgroep 11 oktober: link verslaglegging<br>• Juridische werkgroep 11 oktober: link verslaglegging<br>• Functionele werkgroep 18 september: link verslaglegging<br>• Technische werkgroep 18 september: link verslaglegging<br>• Juridische werkgroep 18 september: link verslaglegging | | |
| | 04 juli 2023 | De opmerkingen die zijn gemaakt op de vorige versie van het afsprakenstelsel en het resultaat van de publieke review zijn verwerkt:<br>De verwerkte schriftelijke review: link.<br>Discussiepunten Tech-Xperiment publieke review: link.<br>Discussiepunten van de functionele publieke review: link.<br>Discussiepunten van de juridische publieke review: link | BESCHIK... | Afsprakenstelsel DSGO 04 juli 2023 |
| | 26 mei 2023 | Publicatie van het afsprakenstelsel DSGO ten behoeve van de publieke review op 15 juni 2023. Onderwerpen toegevoegd:<br>• Wat is een datadienst?<br>• Authenticatie<br>• Autorisatie<br>• Informatiebeveiliging | BESCHIK... | Afsprakenstelsel DSGO 26 mei 2023 |
| | 31 maart 2023 | De eerste publieke publicatie van het afsprakenstelsel DSGO. De opmerkingen die zijn gemaakt op de vorige versie van het afsprakenstelsel en het resultaat van de publieke review zijn verwerkt:<br>De verwerkte schriftelijke review: link<br>Discussiepunten van de technische publieke review: link<br>Discussiepunten van de functionele publieke review: link.<br>Discussiepunten van de Juridische publieke review: link. | BESCHIK... | Afsprakenstelsel DSGO 31 maart 2023 |
| | 16 februari 2023 | Publicatie van het afsprakenstelsel DSGO ten behoeve van de publieke review van het afsprakenstelsel. | REVIEWED | Afsprakenstelsel DSGO 16 februari 2023 |

# Kern van het Afsprakenstelsel DSGO

In de introductie zijn de aanleiding en doel van het DSGO, en de richtinggevende principes van het afsprakenstelsel gepresenteerd. In dit hoofdstuk wordt hierop voortgeborduurd en wordt de kern van het afsprakenstelsel, datadiensten, hoe datadiensten werken, het rollenmodel en de ondersteunende functionaliteiten die deel uitmaken van het afsprakenstelsel geïntroduceerd.

Het afsprakenstelsel schept de voorwaarde om het aanbieden, vinden en gebruiken van datadiensten schaalbaar, interoperabel en betrouwbaar te maken. Zo kan op basis van het afsprakenstelsel, met ondersteuning van voorzieningen een federatief ecosysteem voor data delen in de gebouwde omgeving ontstaan.

Op het afsprakenstelsel gebaseerde datadiensten maken het mogelijk om op gestandaardiseerde wijze data tussen partijen de delen of data te bewerken (zie Wat is een datadienst? en Hoe werkt een datadienst? voor meer informatie). De datadiensten zijn geen doel op zich, maar kunnen worden ingezet door partijen om waarde te creëren of problemen op te lossen in de gebouwde omgeving. In de onderstaande figuur wordt schematisch weergegeven hoe afspraken over alle BLOFT onderwerpen datadiensten mogelijk maken die kunnen worden gebruikt om waarde te creëren.




Op afspraken gebaseerde datadiensten realiseren waarde in de gebouwde omgeving

Het afsprakenstelsel bevat generieke en specifieke afspraken om een breed scala van datadiensten mogelijk te maken die op hun beurt kunnen worden ingezet voor vele mogelijke oplossingen. Generieke afspraken zijn afspraken die voor alle datadiensten van toepassing zijn. Specifieke afspraken zijn afspraken die vastgelegd zijn voor een gekaderde context binnen het DSGO, en zijn enkel van toepassing op datadiensten binnen die gekaderde context. Dit zijn afspraken die bovenop de generieke functionaliteiten zijn gemaakt om sector-, keten-, of oplossingsspecifieke datadiensten mogelijk te maken.

In de onderliggende pagina's worden de belangrijkste onderwerpen van het afsprakenstelsel geïntroduceerd:

- Wat is een datadienst?
- Hoe werkt een datadienst?
- Het DSGO rollenmodel
- Generiek ondersteunende functionaliteiten
- Specifieke functionaliteiten
- Juridische bepalingen
- Governance

# Wat is een datadienst?

Een datadienst maakt het mogelijk om data te delen tussen een datadienstaanbieder en datadienstgebruiker en/of data te bewerken bij een datadienstaanbieder door een datadienstgebruiker. Allebei met toestemming van de rechthebbende. De pagina Hoe werkt een datadienst? beschrijft het functioneren van een datadienst en het rollenmodel geeft een gedetailleerde beschrijving van de rollen die betrokken zijn bij een datadienst.

Als een partij waarde ziet in data delen en/of bewerken, kunnen ze een datadienst aanbieden en de rol van een datadienstaanbieder invullen. Een datadienstaanbieder kan dan zelf een datadienst definiëren en vervolgens vormgeven en binnen de voorwaarden van het afsprakenstelsel. Vervolgens kan een datadienstaanbieder een dienst implementeren en aanbieden via een kanaal naar keuze, waardoor (potentiële) datadienstgebruikers in staat worden gesteld om de datadienst te gebruiken. Afhankelijk van het doel van de datadienstaanbieder kan de datadienst alle mogelijke data bevatten (het afsprakenstelsel is in de eerste plaats data agnostisch en maakt het mogelijk om met een datadienst alle mogelijke data te delen en/of te bewerken).

## Datadienstdefinitie

Het is de verantwoordelijkheid van een datadienstaanbieder om een datadienst te definiëren en implementeren binnen de kaders van het afsprakenstelsel. De volgende pagina bevat de datadienstdefinitie zoals gebruikt in het DSGO.

- Datadienstdefinitie

# Datadienstdefinitie

Datadiensten gebaseerd op het afsprakenstelsel moeten helder gedefinieerd zijn zodat datadienstaanbieders weten wat nodig is voor implementatie en (potentiële) datadienstgebruikers de beschikbare datadiensten kunnen beoordelen en gebruiken. De datadienstdefinitie is gebaseerd op de Data Catalog Vocabulary (DCAT), een open standaard aanbevolen door het Forum voor Standaardisatie, en de Data Sharing Canvas.

:Quotes:

**Bron:** DCAT v3 - Abstract

Data Catalog Vocabulary (DCAT) is an RDF vocabulary designed to facilitate interoperability between data catalogs published on the Web. This document defines the schema and provides examples for its use.

DCAT enables a publisher to describe datasets and data services in a catalog using a standard model and vocabulary that facilitates the consumption and aggregation of metadata from multiple catalogs. This can increase the discoverability of datasets and data services.

De onderstaande tabel geeft een overzicht van de elementen die deel uitmaken van een datadienstdefinitie in het afsprakenstelsel. Het doel van deze tabel is het expliciet maken van alle elementen die nodig zijn voor een duidelijk gedefinieerde datadienst.

| Element | Beschrijving |
|---|---|
| Datadienst titel | De titel van de datadienst |
| Datadienst beschrijving | Een korte beschrijving van de datadienst en het doel ervan |
| Versie | Het versienummer van de datadienst |
| Datadienstaanbieder naam | De naam van de datadienstaanbieder |
| Datadienstaanbieder identifier | Het EORI-nummer van de datadienstaanbieder dat kan worden gebruikt om de datadienstaanbieder te identificeren |
| Datadienstaanbieder contactpunt | Contactinformatie voor de datadienstaanbieder (bv. een e-mailadres of telefoonnummer) |
| Endpoint beschrijving | Een beschrijving van het API endpoint dat door de datadienst wordt gebruikt, inclusief de resources, operaties en file formats ervan (bv. beschreven in YAML-formaat) |
| Endpoint URL | De URL die wordt gebruikt om toegang te krijgen tot de datadienst |
| Taal | De natuurlijke taal die door de datadienst wordt gebruikt (bv. Nederlands, Engels) |
| Semantisch data model | Een (verwijzing naar een) gevestigde standaard die het model, schema, ontologie, view of profiel waaraan de data gebruikt in de datadienst aan voldoet (opmerking: er kunnen meerdere verwijzingen zijn) |
| Betrouwbaarheidsniveaus | Vereist betrouwbaarheidsniveau van de identificatie van datadienstgebruikers die nodig is voor gebruik van de datadienst |
| Beveiligingsniveau | Vereist niveau van beveiliging van de datadienst |
| Toegangscontroleregels | Beleid of richtlijnen waar aan moet worden voldaan voordat er gebruik kan worden gemaakt van de datadienst (bv. de noodzaak van een certificering, of kennis van een ordernummer) |
| Verplichtingen en advies | Beleid of richtlijnen waar aan moet worden voldaan nadat er gebruik is gemaakt van de datadienst (bv. de gebruiksomvang, het beleid inzake gegevensbewaring en |

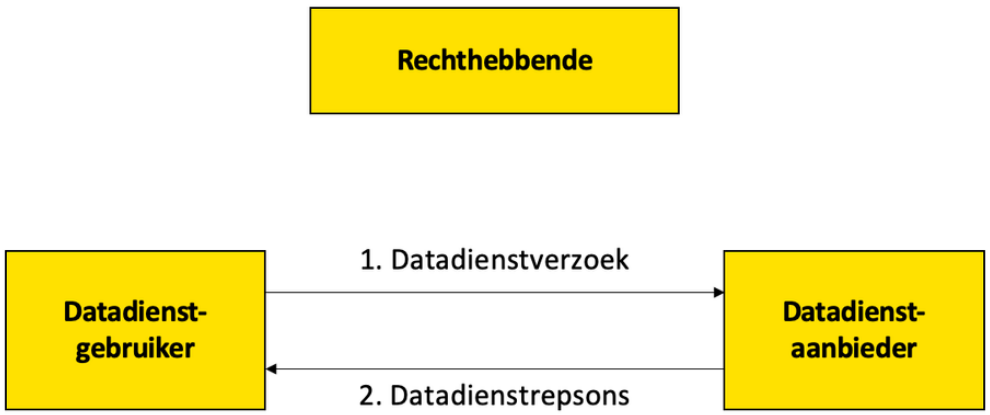
| | |
|---|---|
| | rapportagevereisten) |
| Service level agreements (SLAs) | Alle service level agreements over de dienstverlening of prestatiegaranties gerelateerd aan de datadienst.(bv. garanties inzake uptime of reactietijd) |

**Merk op,** het afsprakenstelsel is in ontwikkeling, in een volgende versie zullen de elementen van de datadienstdefinitie worden gedetailleerd.

# Hoe werkt een datadienst?

Een datadienst maakt het mogelijk om data te delen tussen een datadienstaanbieder en datadienstgebruiker en/of data te bewerken bij een datadienstaanbieder door een datadienstgebruiker. Allebei met toestemming van de rechthebbende. Het rollenmodel geeft een gedetailleerde beschrijving van de rollen die betrokken zijn bij een datadienst.

In de onderstaande figuur worden de generieke interacties voor het uitvoeren van een datadienst weergegeven en in de tabel worden de acties beschreven.




Generiek patroon voor een datadienst

| # | Actie | Omschrijving |
|---|---|---|
| 1 | Datadienstverzoek | De datadienstgebruiker initieert de datadienst door middel van een datadienstverzoek naar de datadienstaanbieder. |
| 2 | Datadienstrespons | De datadienstaanbieder toetst het datadienstverzoek tegen het autorisatiebeleid van de datadienst en stuurt een geschikte response naar de datadienstgebruiker. In het geval van een positieve toets, inclusief het resultaat van de datadienst. |

Volgens het afsprakenstelsel wordt data in een datadienst als resources beschikbaar gesteld. Een resource is een object met een type, bijbehorende data, relaties met andere resources en enkele operaties om deze te bewerken. Een datadienst krijgt vervolgens voor machine-to-machine interacties vorm via API's (Application Programming Interface), en voor human-to-machine interacties vorm via een applicatie, waarmee een operatie op de data resources uitgevoerd wordt. Applicaties voor human-to-machine interacties zijn de verantwoordelijkheid van de desbetreffende partijen, en niet in scope voor het DSGO.

Zie RESTful API's voor een complete introductie van API's en resources voor machine-to-machine interacties. Er zijn vier basisoperaties mogelijk in een datadienst om data delen en/of data bewerken mogelijk te maken. Deze vier operaties worden samengevat in de afkorting CRUD en gepresenteerd in de volgende tabel.

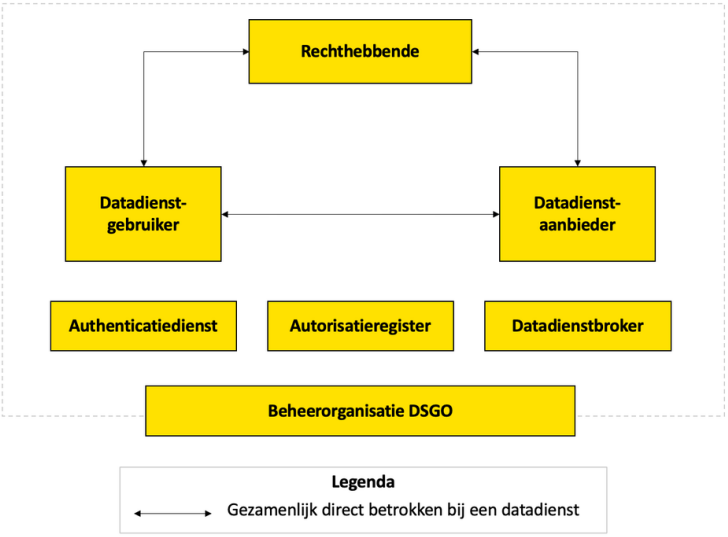
| Operatie | Beschrijving |
|---|---|
| **C**reate | De datadienstgebruiker stuurt data naar de datadienstaanbieder die op basis hiervan een data resource aanmaakt. |

| | |
|---|---|
| **R**ead | De datadienstgebruiker ontvangt de gevraagde data resource van de datadienstaanbieder. |
| **U**pdate | De datadienstgebruiker stuurt data naar de datadienstaanbieder die op basis hiervan een data resource bijwerkt. |
| **D**elete | De datadienstgebruiker verzoekt de datadienstaanbieder om een data resource te verwijderen. De datadienstaanbieder verwijdert de data resource. |

De DSGO structuur voor API's die gebruikt kunnen worden in een datadienst worden hier verder beschreven. Om een datadienst te vinden en conform het DSGO te gebruiken zijn nog een aantal generieke ondersteunende functionaliteiten nodig.

## Het DSGO rollenmodel

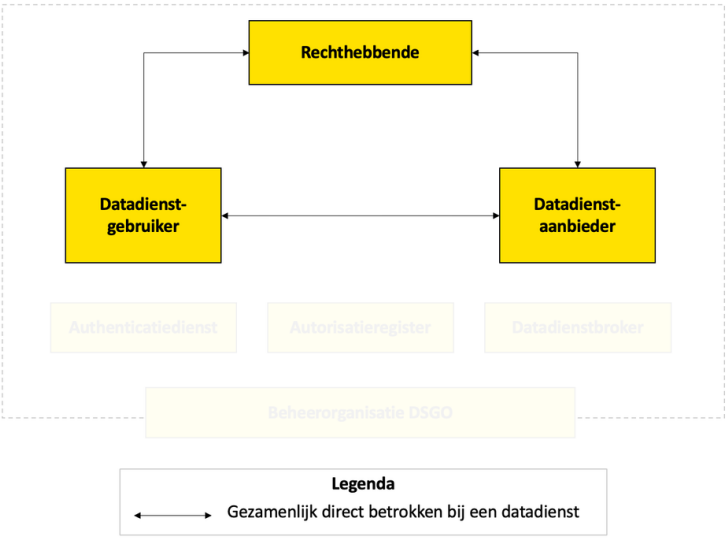
Om het DSGO correct te laten functioneren zijn er verschillende rollen die vervuld moeten worden. Een overzicht van het rollenmodel met alle gedefinieerde rollen is weergegeven in het figuur hieronder:




Rollenmodel van het DSGO

## Sleutelrollen

Bij elke datadienst zijn de drie sleutelrollen direct betrokken, de datadienstaanbieder, de datadienstgebruiker en de rechthebbende. Elke partij in de gebouwde omgeving kan deze rollen vervullen volgens het afsprakenstelsel om datadiensten te leveren, af te nemen, of de rechten over de data te beheren.

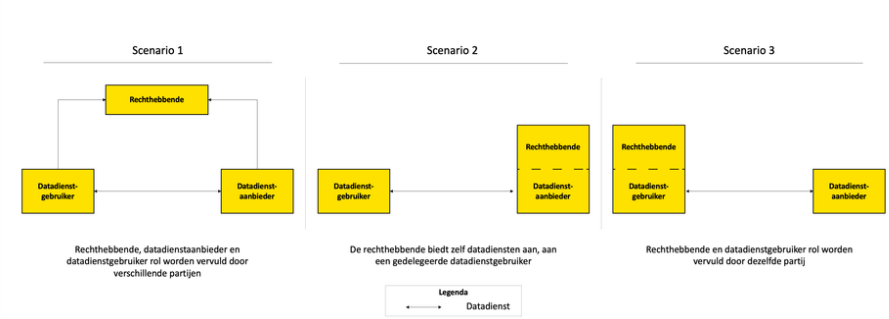



Sleutelrollen van het DSGO

| Rol | Omschrijving | Opmerking |
|---|---|---|
| Datadienst-aanbieder | De datadienstaanbieder is verantwoordelijk voor het definiëren van één of meer datadiensten en deze aan te bieden en leveren conform het afsprakenstelsel en haar datadienstdefinitie. | Elke partij in de gebouwde omgeving kan de rol van een datadienstaanbieder innemen in het DSGO indien ze aan de afspraken voor deze rol voldoen. Datadienstaanbieders moeten deelnemen aan het DSGO, en sluiten bij het toetreden een deelnameovereenkomst met de beheerorganisatie. |
| Datadienst-gebruiker | De datadienstgebruiker is bij het afnemen van een datadienst verantwoordelijk voor het voldoen aan de voorwaarden, verplichtingen en mogelijke delegatie voorwaarden van de datadienst conform de datadienstdefinitie. | Elke partij in de gebouwde omgeving kan de rol van een datadienstgebruiker innemen in het DSGO indien ze aan de afspraken voor deze rol afspraken voldoen. Datadienstgebruikers kunnen deelnemen aan het DSGO, of worden indirect verbonden |

| | | |
|---|---|---|
| | | aan het DSGO middels bilaterale contractuele afspraken met datadienstaanbieders. |
| Rechthebbende | De rechthebbende heeft gebruiksrechten over data en heeft zeggenschap over het gebruikersrecht van derde partijen betreffend die data | De rol van rechthebbende wordt vervuld door de partij die volgens wet- en regelgeving en/of contractuele afspraken gebruikersrechten en zeggenschap heeft over data. De rechthebbende kan ervoor kiezen om gebruik te maken van deze rechten. Wanneer wet- en regelgeving over desbetreffende data ontbreekt en er geen contractuele afspraken zijn is in praktijk vaak de partij waarbij data opgeslagen is rechthebbende.<br><br>Er kunnen meerdere entiteiten rechthebbend zijn over dezelfde data. |

Een partij kan een of meerdere rollen invullen bij het uitvoeren van een datadienst. Bij een andere datadienst kunnen dezelfde entiteiten een andere rol innemen. Een voorbeeld hiervan is gevisualiseerd in het de scenario's hieronder:




Eén partij kan gelijktijdig meerdere rollen vervullen

**Voorbeeld** van mogelijke invullingen van de rollen.

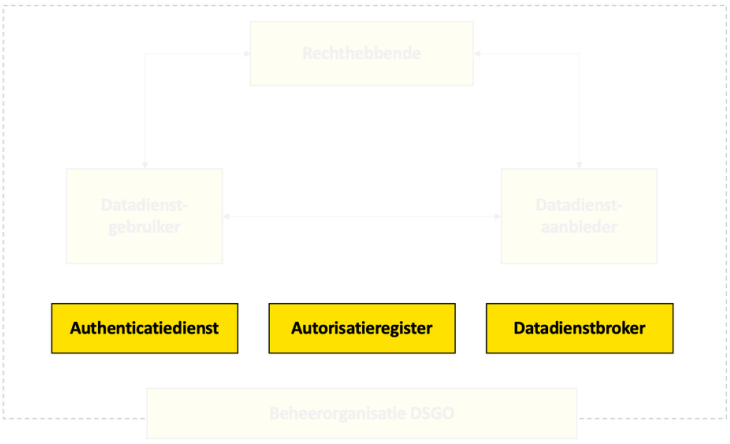
**Scenario 1:** Wanneer productinformatie bij een leverancier is opgeslagen kan de leverancier als datadienstaanbieder een datadienst met productinformatie (bijvoorbeeld de classificatie gegevens) aanbieden aan een aannemer, de datadienstgebruiker. Dit terwijl de fabrikant rechthebbende is over de productinformatie in die datadienst.

**Scenario 2:** Wanneer de fabrikant, als datadienstaanbieder, productinformatie direct aanbiedt aan de aannemer, de datadienstgebruiker, is de fabrikant zowel datadienstaanbieder als rechthebbende.

**Scenario 3:** Het is ook mogelijk dat de leverancier, als datadienstaanbieder, aanvullende productinformatie aanbiedt (bijvoorbeeld de aannemer specifieke verkoopcondities) aan de aannemer, de datadienstgebruiker. De aannemer is dan zowel datadienstgebruiker als rechthebbende.

## Marktvoorzieningen

De rollen van authenticatiedienst, autorisatieregister en datadienstbroker zijn marktvoorzieningen en zijn optioneel ondersteunend bij het uitvoeren van datadiensten. De rol van een marktvoorziening wordt vervuld door marktpartijen in de gebouwde omgeving die voor de desbetreffende rol aan de vereisten voldoen. Marktvoorzieningen moeten gecertificeerd zijn en staan onder toezicht van de beheerorganisatie.



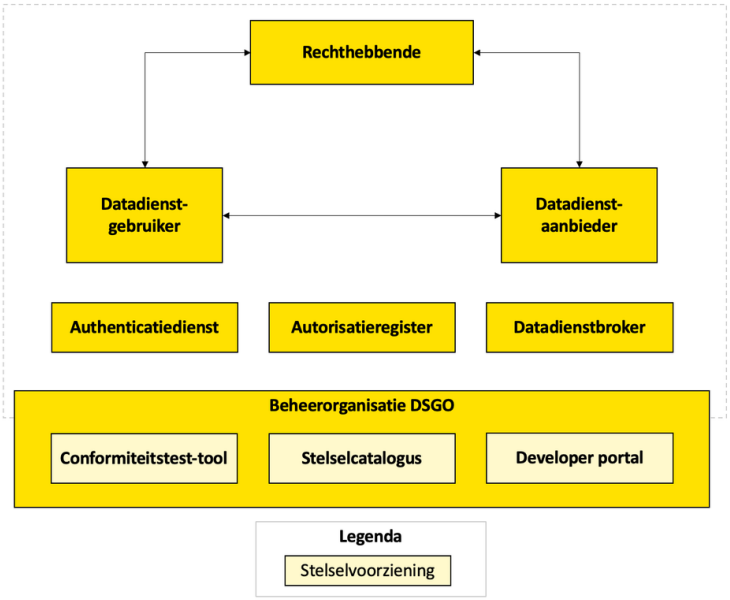

Marktvoorzieningen in het DSGO

| Rol | Omschrijving | Opmerking |
|---|---|---|
| Authenticatie-dienst | Een authenticatiedienst is een onafhankelijke, gecertificeerde partij die diensten aanbiedt voor het creëren, onderhouden, beheren en valideren van identiteiten van natuurlijke personen | Elke partij in de gebouwde omgeving kan de rol van een authenticatiedienst innemen in het DSGO indien ze aan de afspraken voor deze rol voldoen. Authenticatiediensten worden gecertificeerd en nemen deel aan het DSGO. In een datadienst is het gebruik van een authenticatiedienst enkel nodig wanneer een datadienst om een |

| | | |
|---|---|---|
| | (mensen) tijdens het gebruik van datadiensten en/of het registreren van autorisaties. Een authenticatiedienst is een optionele rol en is niet bij elke datadienst betrokken. | natuurlijk persoon gaat en de datadienstaanbieder zelf deze functionaliteit niet biedt. |
| Autorisatie-register | Een autorisatieregister is een onafhankelijke, gecertificeerde partij die diensten aanbiedt voor het registeren, beheren en ontsluiten van delegaties van rechthebbenden aan derden, zodat derden toegang kunnen krijgen tot een datadienst. Een autorisatieregister is een optionele rol en is niet bij elke datadienst betrokken. | Elke partij in de gebouwde omgeving kan de rol van een autorisatieregister innemen in het DSGO indien ze aan afspraken voor deze rol voldoen. Autorisatieregisters moeten worden gecertificeerd en nemen deel aan het DSGO.<br><br>In een datadienst is het gebruik van een autorisatieregister enkel nodig wanneer er spraken is van delegatie van rechten voor het registreren van delegaties. Alternatieven voor het registeren delegaties zijn:<br>• De rechthebbende die zelf haar delegaties beheert en beschikbaar stelt aan de datadienstaanbieder<br>• De rechthebbende die haar delegaties direct bij de datadienstaanbieder registreert |
| Datadienst-broker | Een datadienstbroker is een onafhankelijk gecertificeerde partij die bij de uitvoering van een datadienst optreedt als (technisch) dienstverlener namens een datadienstaanbieder of een datadienstgebruiker. Een datadienstbroker is een optionele rol en is niet bij elke datadienst betrokken. | Elke partij in de gebouwde omgeving kan de rol van een datadienstbroker innemen in het DSGO indien ze aan de afspraken voor deze rol voldoen. Datadienstbrokers moeten worden gecertificeerd en nemen deel aan het DSGO.<br><br>Het gebruik van een datadienstbroker is optioneel voor datadienstaanbieders en datadienstgebruikers, datadienstaanbieders en datadienstgebruikers kunnen kiezen om gebruik te maken van een datadienstbroker wanneer ze de technische uitvoering van de datadienst willen laten uitvoeren door een vertrouwde partij. Datadienstbrokers moeten een contractuele overeenkomst hebben met de partijen namens wie de datadienstbroker optreedt. |

## Beheerorganisatie DSGO

De rol van de beheerorganisatie DSGO is verantwoordelijk voor het (laten) uitvoeren van diverse activiteiten om continuïteit van het DSGO te borgen. Als onderdeel van het beheren van het DSGO valt het leveren en beheren van de stelselvoorzieningen.




De beheerorganisatie van het DGSO

| Rol | Omschrijving |
|---|---|
| Beheerorganisatie DSGO | De beheerorganisatie is verantwoordelijk het (laten) uitvoeren van de activiteiten rondom beheer, adoptie en doorontwikkeling van het DSGO. |

### Stelselvoorzieningen

De beheerorganisatie levert de stelselvoorzieningen van het DSGO. Dit zijn de developer portal, conformiteitstest-tool en stelselcatalogus welke partijen ondersteunen bij de voorbereiding en uitvoering van datadiensten.

| Stelselvoorziening | Omschrijving | Opmerking |
|---|---|---|
| Developer portal | De developer portal is een online interface waar ontwikkelaars documentatie tools en middelen kunnen vinden om effectief gebruik te maken van de DSGO specificaties, waardoor ze gemakkelijk softwaretoepassingen kunnen bouwen en integreren | De beheerorganisatie levert de DSGO developer portal als stelselvoorziening. |
| Conformiteitstest-tool | De conformiteitstest-tool is een software hulpmiddel dat is ontworpen om de beheerorganisatie DSGO (i.o.) te laten verifiëren of de implementatie van een API voldoet aan de gestelde DSGO generieke afspraken | De beheerorganisatie levert de DSGO conformiteitstest-tool als stelselvoorziening die wordt gebruikt bij het testen en certificeren van datadiensten. |
| Stelselcatalogus | De stelselcatalogus biedt een overzicht van deelnemers en datadiensten in het DSGO om andere partijen de benodigde informatie te bieden voor het vinden en uitvoeren van datadiensten. | De beheerorganisatie levert de DSGO stelselcatalogus als stelselvoorziening die wordt gebruikt voor het registeren en vinden van partijen en datadiensten. |

**Merk op**, in de doorontwikkeling van het afsprakenstelsel kunnen aanvullende rollen die nodig worden geacht worden toegevoegd aan het rollenmodel.

# Rechten en plichten

De verschillende rollen binnen het DSGO hebben rechten en plichten die ze respectievelijk toekomen, en moeten nakomen. Rechten en plichten staan expliciet in het afsprakenstelsel, en zijn aanvullend op eventuele (reeds bestaande) rechten en plichten op basis van geldende (algemene) wetgeving of overeenkomsten. Het staat partijen vrij om onderling additionele rechten en plichten overeen te komen bij het uitvoeren van een datadienst zolang dit niet in strijd is met de rechten en plichten van en voortvloeiend uit het DSGO.

De werking van het DSGO en het opereren van de verschillende rollen worden middels deze rechten en plichten beschreven. De rechten en plichten worden in het afsprakenstelsel gespecificeerd naar praktische en gedetailleerdere afspraken. Partijen zijn vrij om elke rol binnen het DSGO te vervullen en mogen meerdere rollen vervullen indien ze (blijvend) aan de plichten van die rol(len) voldoen.

**Rechten:** Wat de rol mag doen en verwachten binnen het DSGO

**Plichten:** Wat de verantwoordelijkheden zijn en wat er van de rol verwacht wordt binnen het DSGO

Algemene rechten en plichten welke gelden voor de sleutelrollen en marktvoorzieningen worden hieronder gepresenteerd, rechten en plichten die gelden voor een specifieke rol zijn verder gedetailleerd op onderliggende pagina's:

- Datadienstaanbieder
- Datadienstgebruiker
- Rechthebbende
- Authenticatiedienst
- Autorisatieregister
- Datadienstbroker
- Beheerorganisatie DSGO

# Algemene rechten en plichten

## Rechten

- Een partij is vrij om één of meerdere rollen binnen het DSGO te vervullen indien ze aan de plichten van de desbetreffende rol voldoen (zie Het DSGO rollenmodel)
- Een partij mag een aanvullende overeenkomst sluiten met een wederpartij voor het aangaan van een datadienst zolang dit geen conflict met het afsprakenstelsel oplevert
- Een partij heeft het recht om compensatie te vragen aan andere partijen voor haar activiteiten in het DSGO
- Een partij mag haar activiteiten uitbesteden onder de volgende voorwaarden:
  - Als een partij haar activiteiten uitbesteed aan een marktvoorziening, dan is de marktvoorziening verantwoordelijk voor het correct functioneren van die activiteiten conform het afsprakenstelsel (zie Marktvoorzieningen)
  - Als een partij haar activiteiten uitbesteed aan andere partijen blijft de uitbestedende partij verantwoordelijk voor het correct functioneren van haar activiteiten conform het afsprakenstelsel
- Een partij heeft het recht tijdig op de hoogte te worden gebracht van wijzigingen in het afsprakenstelsel (zie Change en release management)

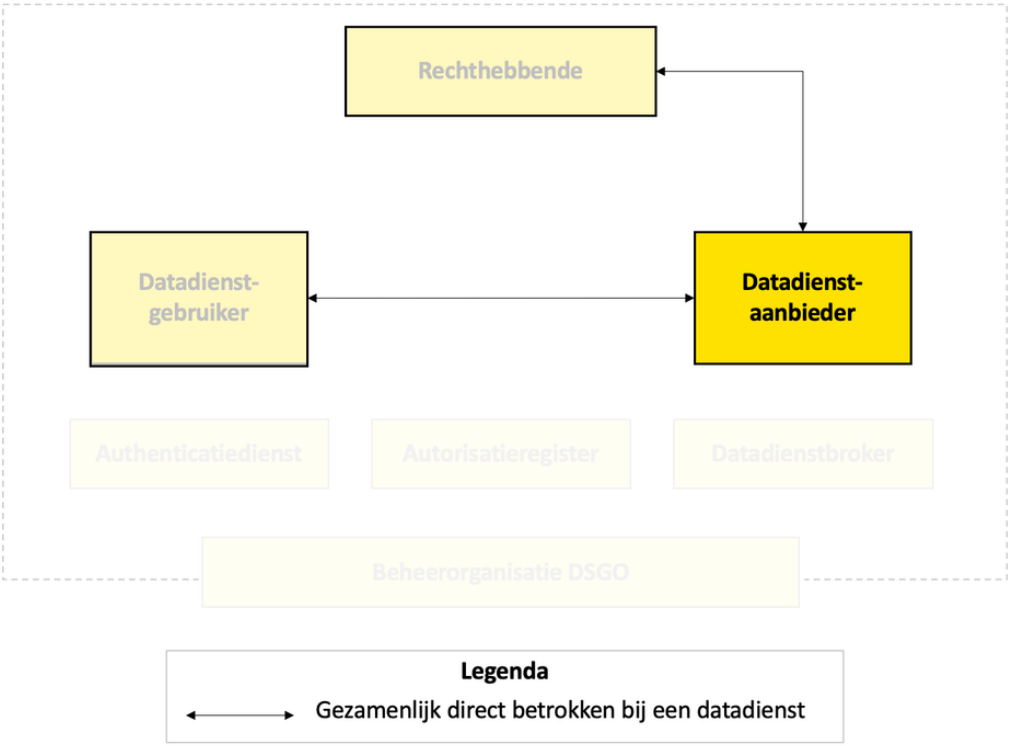
## Plichten

- Een partij moet blijvend handelen conform het afsprakenstelsel en zich inspannen aanpassingen in het afsprakenstelsel door te voeren (zie Generieke afspraken, Specifieke afspraken en Change en release management)
- Een partij dient, bij haar activiteiten binnen het DSGO, te handelen conform geldende wet- en regelgeving (zie Juridische context)

- Een partij dient voorzieningen te gebruiken conform het afsprakenstelsel en de voorwaarden van de desbetreffende voorziening (zie Marktvoorzieningen & Stelselvoorzieningen)
- Een partij informeert de beheerorganisatie DSGO en betrokken partijen bij incidenten binnen het DGSO (fouten, het vermoeden van het doelbewust onrechtmatig handelen, etc) wanneer zij hiervan kennis heeft genomen (zie Toezicht en handhaving en Beheerorganisatie DSGO)

# Datadienstaanbieder

De datadienstaanbieder is verantwoordelijk voor het definiëren van één of meer datadiensten en deze aan te bieden en leveren conform het afsprakenstelsel en haar datadienstdefinitie. Voor de datadienstaanbieder gelden de algemene rechten en plichten en de rol specifieke rechten en plichten hieronder.




De datadienstaanbieder in het DSGO rollenmodel

## Rechten

- Een datadienstaanbieder mag datadiensten aanbieden onder de voorwaarden van het afsprakenstelsel. De datadienstaanbieder is vrij om binnen deze voorwaarden haar datadienst te definiëren (zie Wat is een datadienst):
  - Een datadienstaanbieder is vrij de inhoud en functionaliteit van haar datadienst te bepalen
  - Een datadienstaanbieder is vrij voorwaarden aan het gebruik van haar datadienst te stellen en een licentie aan de datadienstdefinitie toe te voegen (zie Juridische bepalingen en Datadienstdefinitie)
- Een datadienstaanbieder mag bepalen welke (informatie over) datadienst(en) in de stelselcatalogus wordt geregistreerd (zie Stelselvoorzieningen)
- Een datadienstaanbieder heeft recht op inspraak bij de (door)ontwikkeling van het afsprakenstelsel (zie Governance)

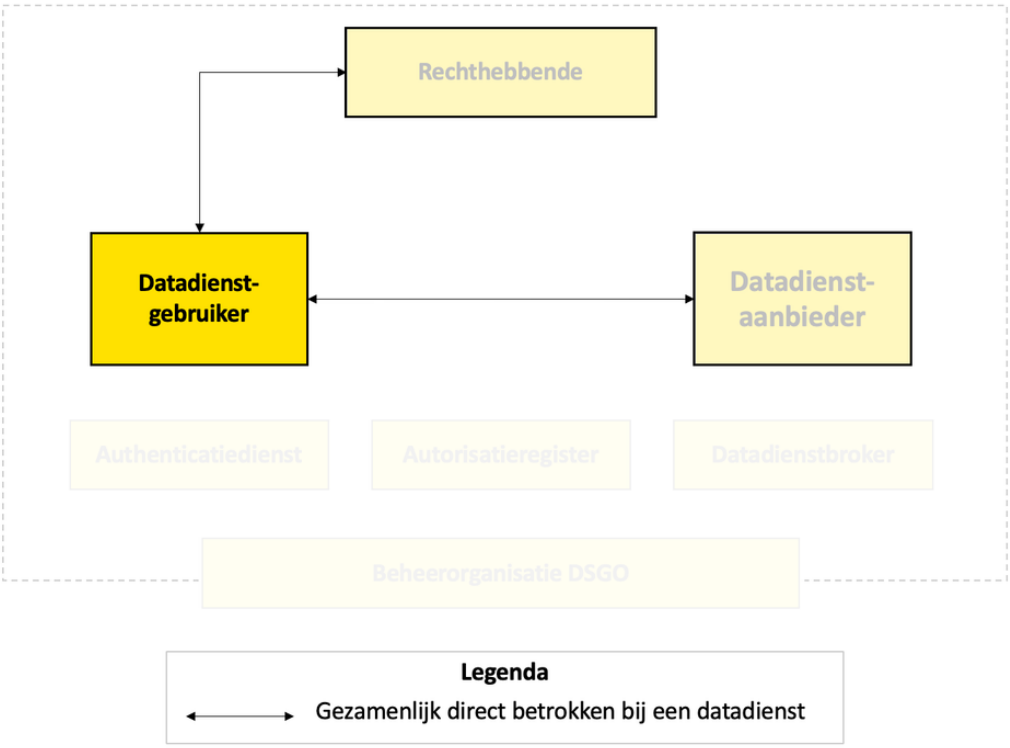
## Plichten

- Een datadienstaanbieder is deelnemer en heeft een deelnameovereenkomst met de beheerorganisatie DSGO (zie Juridische bepalingen en Governance)
- Een datadienstaanbieder moet de gebruiksvoorwaarde van het DSGO van toepassing verklaren bij het gebruik van haar datadienst (zie Juridische bepalingen)

- Een datadienstaanbieder is verantwoordelijk voor het aanbieden van de datadienst conform het afsprakenstelsel (zie Wat is een datadienst). Dit betekent o.a. dat de datadienst:
  - Gebaseerd is op RESTful APIs conform het afsprakenstelsel (zie Generieke Technische Standaarden en API specificaties)
  - Identificatie, authenticatie en autorisatie uitvoert conform het afsprakenstelsel en vereisten van marktvoorzieningen (zie Identificatie, Authenticatie en Autorisatie)
  - Toegang geeft tot (bewerking van) data waar de rechthebbende datadienstgebruiker, of de gedelegeerde datadienstgebruiker, rechten over heeft (zie Autorisatie)
- Een datadienstaanbieder is verantwoordelijk om te handelen conform het afsprakenstelsel in de context van datadiensten. Dit betekent o.a. dat een datadienstaanbieder:
  - Haar organisatie zo heeft ingericht dat processen in de context van datadiensten conform het afsprakenstelsel worden uitgevoerd (zie Service Level Agreements en Operationele processen)
  - Handelt bewust naar de informatiebeveiligingsrisico's die ze neemt in de context van datadiensten die ze aanbiedt (zie Informatiebeveiliging)
- Een datadienstaanbieder communiceert informatie over en voorwaarden voor het gebruik van haar datadienst(en) conform de datadienstdefinitie, al dan niet via de stelselcatalogus (zie Datadienstdefinitie en Stelselvoorzieningen)
  - Een datadienstaanbieder zou richting rechthebbendden en/of datadienstgebruikers moeten communiceren wanneer een datadienst wijzigt
- Een datadienstaanbieder wordt geacht te weten wie de rechthebbenden zijn op de data(diensten) die zij aanbiedt (zie Het DSGO rollenmodel). Hoe de datadienstaanbieder dit achterhaalt is buiten scope van het DSGO

# Datadienstgebruiker

De datadienstgebruiker is bij het afnemen van een datadienst verantwoordelijk voor het voldoen aan de voorwaarden, verplichtingen en mogelijke delegatie voorwaarden van de datadienst conform de datadienstdefinitie. Een datadienstgebruiker kan dat als zij ook de rol van rechthebbende vervult (rechthebbende datadienstgebruiker) of als deze partij gedelegeerde rechten heeft van de rechthebbende (gedelegeerde datadienstgebruiker). Voor de datadienstgebruiker gelden de algemene rechten en plichten en de rol specifieke rechten en plichten hieronder.




De datadienstgebruiker in het DSGO rollenmodel

## Rechten

- Een datadienstgebruiker mag gebruik maken van datadiensten als zij voldoet aan de voorwaarden uit het afsprakenstelsel en de betreffende datadienst (zie Wat is een datadienst en Autorisatie)
- Een datadienstgebruiker mag verwachten dat datadiensten binnen het DSGO voldoen aan de afspraken in het afsprakenstelsel (zie Generieke afspraken en Specifieke afspraken)
- Een datadienstgebruiker heeft recht op het inzien van de datadienstdefinitie van datadiensten waarvan zij toestemming heeft gekregen van de datadienstaanbieder (zie Datadienstdefinitie)

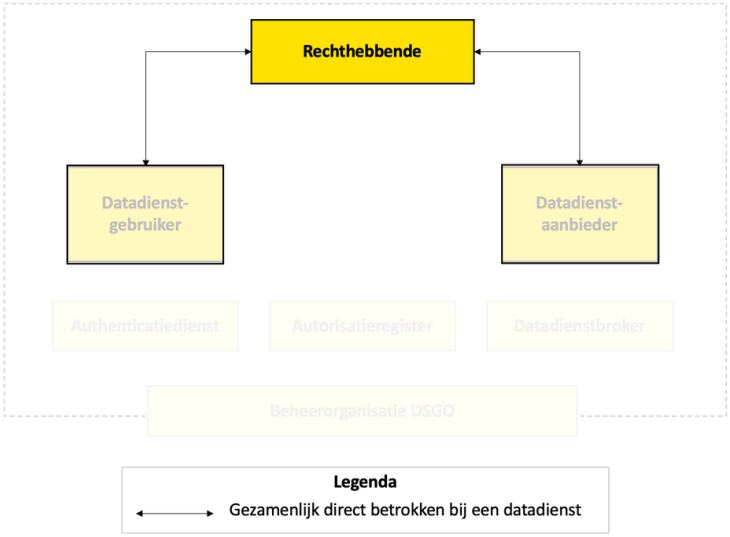
## Plichten

- Een datadienstgebruiker dient akkoord te gaan met de afspraken die voor haar specifieke rol gelden wanneer zij een datadienst binnen het DSGO afneemt (zie Juridische bepalingen), een datadienstgebruiker kan dit doen door:
  - Een bilaterale overeenkomst met een datadienstaanbieder aan te gaan waar in de gebruikersvoorwaarden van het DSGO van toepassing worden verklaard of;
  - Wanneer ze al een deelnameovereenkomst gesloten heeft met de beheerorganisatie, omdat ze een andere rol vervult in het DSGO. In de deelnameovereenkomst wordt het afsprakenstelsel van toepassing verklaard.

- Een datadienstgebruiker dient datadiensten af te nemen conform de datadienstdefinitie (zie Datadienstdefinitie)
- Een datadienstgebruiker handelt bewust naar de informatiebeveiligingsrisico's die ze neemt in de context van datadiensten die ze afneemt (zie Informatiebeveiliging)
- Een datadienstgebruiker gebruikt na het afnemen van een datadienst de data gerelateerd aan de datadienst conform de datadienstdefinitie inclusief de bijhorende licentie (zie Juridische bepalingen en Datadienstdefinitie)

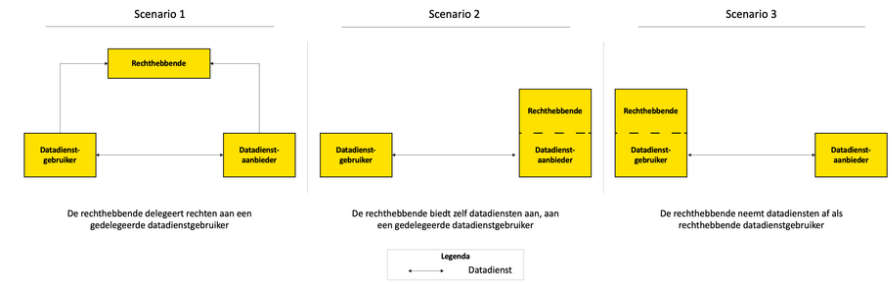
# Rechthebbende

De rechthebbende heeft gebruiksrechten over data en heeft zeggenschap over het gebruikersrecht van derde partijen betreffend die data. Voor de rechthebbende gelden de algemene rechten en plichten en de rol-specifieke rechten en plichten hieronder.




De rechthebbende in het DSGO rollenmodel

De rechthebbende kan bij uitvoering van een datadienst verschillende rollen innemen afhankelijk van het scenario. In elk scenario heeft de rechthebbende verschillende rechten die ze kan uitoefenen. Zie de verschillende scenario's in het figuur hieronder.




De verschillende scenario's in welke een rechthebbende betrokken kan zijn bij een datadienst

## Rechten

- **Scenario 1:** Een rechthebbende mag binnen de kaders van de datadienst (een deel van) haar rechten delegeren, bepalen waar haar delegaties geregistreerd worden en daar voorwaarden (bijvoorbeeld tegenprestaties of licenties) aan stellen:
  - Een rechthebbende mag haar delegaties in haar eigen systemen beheren en vanuit daar ontsluiten
  - Wanneer een datadienstaanbieder daar faciliteiten voor biedt, mag een rechthebbende haar delegaties bij de datadienstaanbieder laten beheren
  - Een rechthebbende mag haar delegaties in een autorisatieregister laten beheren
- **Scenario 2:** Een rechthebbende mag data waar zij rechten op heeft ontsluiten als datadienstaanbieder (zie Wat is een Datadienst)
- **Scenario 3:** Een rechthebbende heeft als rechthebbende datadienstgebruiker zelf recht op toegang tot (bewerking van) data binnen de kaders van de datadienst (zie Wat is een Datadienst en Autorisatie)

## Plichten

- Een rechthebbende dient akkoord te gaan met de afspraken die voor haar specifieke rol gelden wanneer zij een datadienst binnen het DSGO afneemt. Afhankelijk van het scenario in welke de rechthebbende betrokken is bij een datadienst en de keuze voor de registratie van delegaties zijn hier verschillende mogelijkheden voor (zie Juridische bepalingen en Delegaties). Deze mogelijkheden worden geduid in de tabel onderaan deze pagina:
- Een rechthebbende moet eventuele delegaties actief beheren en staat in voor de juistheid van de geregistreerde delegatie (zie Delegaties)

| **Betrokkenheid van de rechthebbende** | **Scenario 1** | **Scenario 2** | **Scenario 3** |
|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| Keuze voor delegatie registratie | Delegatie registratie in de rechthebbende haar eigen systemen | Delegatie registratie bij de datadienstaanbieder | Delegatie registratie in een autorisatieregister | n.v.t. | n.v.t. |
| Wijze van akkoord gaan met voor de rechthebbende geldende afspraken | Rechthebbende is deelnemer en heeft een deelnameovereenkomst met de beheerorganisatie DSGO | Rechthebbende heeft een bilaterale overeenkomst met een datadienstaanbieder waar de gebruikersvoorwaarden van het DSGO van toepassing worden verklaard | Rechthebbende heeft een bilaterale overeenkomst met een autorisatieregister waar de gebruikersvoorwaarden van het DSGO van toepassing worden verklaard | Rechthebbende is deelnemer en heeft een deelnameovereenkomst met de beheerorganisatie DSGO | Rechthebbende heeft een bilaterale overeenkomst met een datadienstaanbieder waar de gebruikersvoorwaarden van het DSGO van toepassing worden verklaard |

# Authenticatiedienst

Een authenticatiedienst is een onafhankelijke, gecertificeerde partij die diensten aanbiedt voor het creëren, onderhouden, beheren en valideren van identiteiten van natuurlijke personen (mensen) tijdens het gebruik van datadiensten en/of het registreren van autorisaties. Een authenticatiedienst is een optionele rol en is niet bij elke datadienst betrokken. Voor authenticatiediensten gelden de algemene rechten en plichten en de rol-specifieke rechten en plichten hieronder.


Een authenticatiedienst in het DSGO rollenmodel

## Rechten

- Een authenticatiedienst mag diensten aanbieden om identificatie, authenticatie en autorisatie van natuurlijke personen, op het Level of Assurance (LoA) waarop ze gecertificeerd zijn, mogelijk te maken (zie Identificatie, Authenticatie en Autorisatie), dit betekent o.a. dat een authenticatiedienst:
  - (Namens organisaties) identificerende kenmerken en kwalificaties mag uitgeven aan natuurlijke personen en deze mag beheren
  - Natuurlijke personen mag authenticeren, en vaststellen welke rechten aan hen zijn gedelegeerd door hun organisatie
  - Rechten (delegaties) die natuurlijke personen krijgen om namens hun organisatie te handelen mag beheren
  - Rechten van natuurlijke personen na succesvolle identificatie en authenticatie aan datadienstaanbieders mag verstrekken
- Een authenticatiedienst heeft recht op inspraak bij de (door)ontwikkeling van het afsprakenstelsel (zie Governance)

## Plichten

- Een authenticatiedienst is deelnemer en heeft een deelnameovereenkomst met de beheerorganisatie DSGO (zie Juridische bepalingen en Governance)
- Een authenticatiedienst is verantwoordelijk voor het aanbieden van haar diensten conform het afsprakenstelsel (zie Wat is een datadienst). Dit betekent o.a. dat een authenticatiedienst:
  - Blijvend aan alle eisen die in iSHARE voor Identity Provider gesteld worden voldoet (zie Marktvoorzieningen)
  - Beschikt over een managementsysteem voor informatiebeveiliging dat voldoet aan de vereisten in het afsprakenstelsel en gecertificeerd is door een onafhankelijke en gespecialiseerde partij

- Een authenticatiedienst levert diensten betreft het identificeren, authentiseren van natuurlijke personen ten behoeve van autorisatie conform het afsprakenstelsel (zie Marktvoorzieningen), dit betekent o.a. dat een authenticatiedienst:
  - De datadienstgebruiker een (online) interface biedt om zich te (laten) authenticeren.
  - De datadienstaanbieder en de datadienstgebruiker ondersteunt bij het identificeren, authenticeren en het organiseren van de autorisatie-informatie van een datadienst wanneer dit is opgenomen in de datadienstdefinitie
  - Datadienstgebruikers bij haar laat registreren voordat de authenticatiedienst ondersteunende functionaliteiten gaat uitvoeren bij een datadienst

# Autorisatieregister

Een autorisatieregister is een onafhankelijke, gecertificeerde partij die diensten aanbiedt voor het registeren, beheren en ontsluiten van delegaties van rechthebbenden aan derden, zodat derden toegang kunnen krijgen tot een datadienst. Een autorisatieregister is een optionele rol en is niet bij elke datadienst betrokken. Voor autorisatieregisters gelden de algemene rechten en plichten en de rol-specifieke rechten en plichten hieronder.


Een autorisatieregister in het DSGO rollenmodel

## Rechten

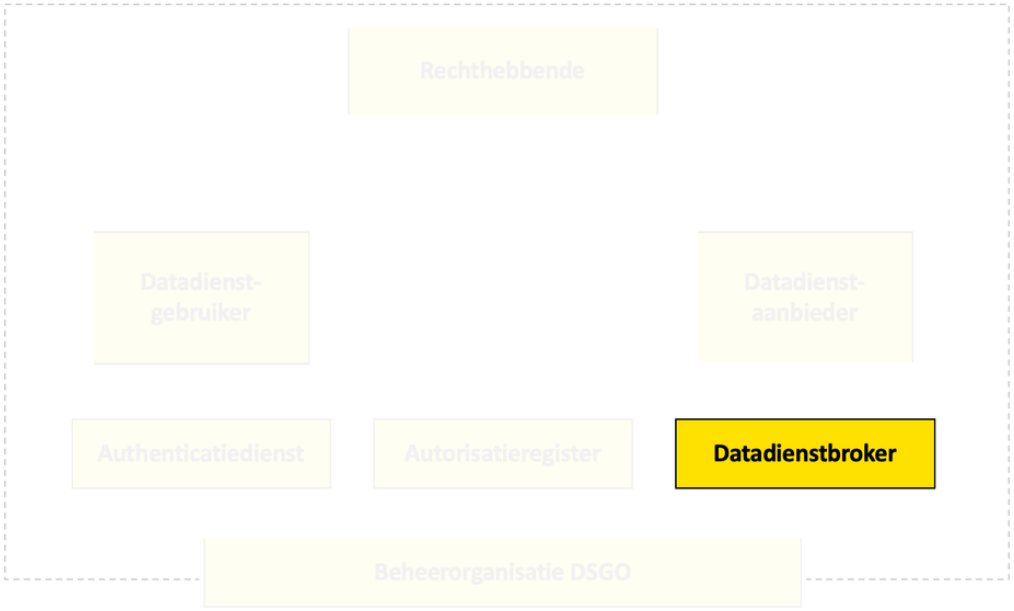
- Een autorisatieregister mag diensten leveren om voor de rechthebbende delegaties te registreren en  te ontsluiten. (zie Autorisatie en Delegatie)
- Een autorisatieregister heeft recht op inspraak bij de (door)ontwikkeling van het afsprakenstelsel (zie Governance)

## Plichten

- Een autorisatieregister is deelnemer en heeft een deelnameovereenkomst met de beheerorganisatie DSGO (zie Juridische bepalingen en Governance)
- Een autorisatieregister is verantwoordelijk voor het aanbieden van haar diensten conform het afsprakenstelsel (zie Wat is een datadienst). Dit betekent o.a. dat een autorisatieregister:
  - Blijvend aan alle eisen die in iSHARE voor Authorisation Registry gesteld worden voldoet (zie Marktvoorzieningen)
  - Beschikt over een managementsysteem voor informatiebeveiliging dat voldoet aan de vereisten in het afsprakenstelsel en gecertificeerd is door een onafhankelijke en gespecialiseerde partij
- Een autorisatieregister levert diensten zodat rechthebbende gedelegeerde rechten kan registreren en beheren ter ondersteuning van het autoriseren van datadienstgebruikers (zie Autorisatie), dit betekent o.a. dat een autorisatieregister:
  - De rechthebbende een (online) interface biedt om haar delegaties te beheren
  - Delegatie bewijzen levert t.b.v. het autorisatieproces van de datadienstaanbieder

# Datadienstbroker

Een datadienstbroker is een onafhankelijk gecertificeerde partij die bij de uitvoering van een datadienst optreedt als (technisch) dienstverlener namens een datadienstaanbieder of een datadienstgebruiker. Een datadienstbroker is een optionele rol en is niet bij elke datadienst betrokken. Voor datadienstbrokers gelden de algemene rechten en plichten en de rol specifieke rechten en plichten hieronder.




Een datadienstbroker in het DSGO rollenmodel

## Rechten

- Een datadienstbroker mag optreden namens de datadienstaanbieder en/of datadienstgebruiker (zie Wat is een Datadienst), dit betekent o.a. dat de datadienstbroker:
  - Namens een partij een datadienstverzoek mag versturen en/of ontvangen
  - Namens een partij een datadienstrespons mag versturen en/of ontvangen
- Een datadienstbroker mag additionele diensten aanbieden binnen de context van een datadienst mits dat is overeengekomen met de partij namens wie zij optreedt
- Een datadienstbroker mag verwachten dat datadiensten binnen het DSGO voldoen aan de afspraken in het afsprakenstelsel
- Een datadienstbroker heeft recht op inspraak bij de (door)ontwikkeling van het afsprakenstelsel (zie Governance)

## Plichten

- Een datadienstbroker is deelnemer en heeft een deelnameovereenkomst met de beheerorganisatie DSGO (zie Juridische bepalingen en Governance)
- Een datadienstbroker is verantwoordelijk voor het aanbieden van haar diensten conform het afsprakenstelsel (zie Wat is een datadienst). Dit betekent o.a. dat een datadienstbroker:
  - Beschikt over een managementsysteem voor informatiebeveiliging dat voldoet aan de vereisten in het afsprakenstelsel en gecertificeerd is door een onafhankelijke en gespecialiseerde partij
- Een datadienstbroker heeft een overeenkomst met de partij namens wie zij optreedt

- Een datadienstbroker moet bij iedere datadienst een geldig bewijs kunnen overleggen dat ze van een partij toestemming heeft om namens die partij te mogen handelen:
  - Een datadienstbroker moet een geldig bewijs kunnen overleggen dat ze in de context van de specifieke datadienst handelt
  - Een datadienstbroker moet zich bij iedere datadienst identificeren en authentiseren conform het DSGO (zie Identificatie en Authenticatie)
  - Een datadienstbroker maakt gebruik van de autorisatie en eventueel delegatie van de datadienstgebruiker (zie Autorisatie)

**Merk op**, momenteel zijn er voor de rol van datadienstbroker nog geen afspraken opgesteld. In de doorontwikkeling van het afsprakenstelsel wordt de rol van datadienstbroker verder geconcretiseerd door hier afspraken voor op te stellen. Hierin wordt input van de werkgroep 10 oktober en de publieke review van 16 november meegenomen.

# Beheerorganisatie DSGO

De beheerorganisatie is verantwoordelijk het (laten) uitvoeren van de activiteiten rondom beheer, adoptie en doorontwikkeling van het DSGO.


De beheerorganisatie DSGO in het DSGO rollenmodel

## Rechten

- De beheerorganisatie DSGO is binnen de kaders gesteld in de operationele processen vrij om het DSGO te beheren op een wijze die het vertrouwen tussen, en de interoperabiliteit van, gebruikers ten goede komt (zie Governance), dit betekent o.a. dat de beheerorganisatie DSGO:
  - Partijen toe mag laten treden en mits gewenst mag registreren wanneer ze het (nog te ontwikkelen) toetredingsproces succesvol doorlopen
  - Het recht heeft incidenten op een gepaste manier zelf te beslechten of dit uit te besteden aan een externe incidentencoördinator (zie Toezicht en handhaving)
  - Het recht heeft gepaste handhavende maatregelen te nemen jegens deelnemers die niet conform het DSGO opereren (zie Toezicht en handhaving)
  - Kleinschalige aanpassingen mag maken aan het afsprakenstelsel conform het change en release management proces (zie Change en release management)
  - Stelselvoorzieningen mag (laten) beheren
- De beheerorganisatie DSGO mag activiteiten (laten) uitvoeren waarvan zij denkt dat die de adoptie van het DSGO stimuleren (zie Governance)
- De beheerorganisatie DSGO mag het afsprakenstelsel en stelselvoorzieningen grootschalig (laten) doorontwikkelen conform het change en release management proces (zie Governance en Change en release management)

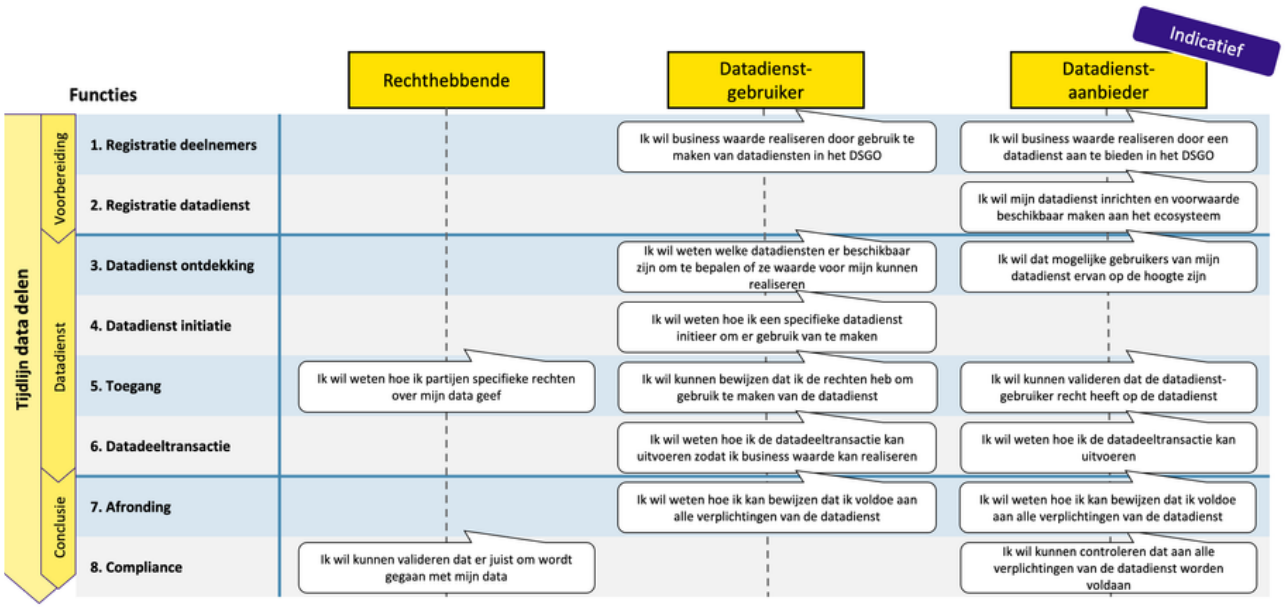
## Plichten

- De beheerorganisatie DSGO beheert het DSGO, stimuleert adoptie van het DSGO en faciliteert doorontwikkeling van het DSGO (zie Governance), dit betekent o.a. dat de beheerorganisatie DSGO
  - Beschikt over een managementsysteem voor informatiebeveiliging dat voldoet aan de vereisten in het afsprakenstelsel en gecertificeerd is door een onafhankelijke en gespecialiseerde partij
  - Toeziet dat potentiële deelnemers bij toetreding aan alle eisen van het nog te ontwikkelen toetredingsproces voldoet
  - Vanuit een neutrale rol geschillen beslecht en besluit om geschillen te escaleren naar een ander (juridisch) orgaan of andere externe partij waar nodig (zie Toezicht en Handhaving)
  - Toeziet op naleving van het DSGO en adequate acties onderneemt jegens andere gebruikers wanneer deze de gemaakte afspraken niet naleven (zie Toezicht en Handhaving)
  - Groot- en kleinschalige ontwikkeling van het DSGO conform het Change Management Proces uitvoert (zie Change en release management)
- De beheerorganisatie doet wat binnen haar kunnen ligt om het interoperabel en vertrouwd functioneren van het DSGO ten alle tijden te waarborgen en de gebruikers van het DSGO daarbij centraal te stellen
- De beheerorganisatie neemt de inspraak van de deelnemers in de daarvoor opgestelde organen mee in de uitvoering van haar taken (zie Governance)
- De beheerorganisatie neemt de richtinggevende principes in acht bij de doorontwikkeling van het DSGO (zie Richtinggevende principes)

**Merk op**, de ontwikkeling en inrichting van de beheerorganisatie DSGO valt onder een separaat project binnen het DSGO-programma en is nog aan verandering onderhevig. Het overzicht van rechten en plichten is daarmee een eerste indicatie

# Generiek ondersteunende functionaliteiten

Er zijn generieke ondersteunende functionaliteiten nodig om de kernfunctionaliteit van een datadienst mogelijk te maken. Deze ondersteunende functionaliteiten bieden geen directe waarde voor de partijen, maar zijn voorwaardelijk om waarde te bieden (bijvoorbeeld door het verzorgen van vertrouwen, infrastructuur en privacy). In de figuur hieronder worden typische uitdagingen van betrokken partijen weergegeven die voor, tijdens en na een datadienst plaats kunnen vinden.




Alle betrokkene hebben uitdagingen op verschillende tijdstippen tijdens het volledige levenscyclus van data delen

Ondersteunende functionaliteiten worden hier verder gedetailleerd:

- Abonnement op een gebeurtenis
- Datadienst ontdekking
- Identificatie, Authenticatie en Autorisatie

Voor alle generieke ondersteunende functionaliteiten zijn generieke afspraken opgesteld.

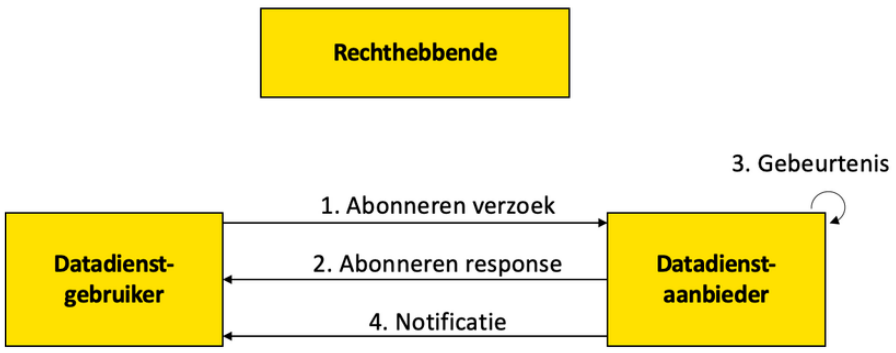
# Abonnement op een gebeurtenis

Een abonnement op een gebeurtenis is een gestandaardiseerde datadienst die de partij (die zich op voorhand heeft geabonneerd op meldingen over een (type) gebeurtenis) inlicht over deze gebeurtenis. Het concept van een abonnement is relevant voor veel partijen in de gebouwde omgeving. Om de werking van abonnementen te formaliseren in het DSGO definieert het afsprakenstelsel een abonnement als een gestandaardiseerde datadienst. Datadienstaanbieders zijn niet verplicht een abonnement te implementeren. Een abonnement speelt een belangrijke rol wanneer een datadienstgebruiker (met toestemming van de rechthebbende) op de hoogte gehouden wil worden van gebeurtenissen (bijvoorbeeld wijzigingen van de brondata) door middel van notificaties van de datadienstaanbieder op bepaalde resources. Deze termen worden in de tabel hieronder beschreven.

| Term | Omschrijving |
|---|---|
| Gebeurtenis | Een identificeerbaar en specifiek voorval zoals gedefinieerd door de datadienstaanbieder. Bijvoorbeeld het wijzigen van de brondata. |
| Abonnement | Een overeenkomst tussen een datadienstaanbieder en een datadienstgebruiker (met toestemming van de rechthebbende) om notificaties te ontvangen over de gedefinieerde gebeurtenissen. |
| Notificaties | Een melding van een gebeurtenis van de datadienstaanbieder, ontvangen door de datadienstgebruiker onder de voorwaarde van een abonnement. |

Het onderstaande figuur illustreert in een interactiemodel hoe een abonnement tot stand komt en hoe notificaties van gebeurtenissen worden doorgegeven.

**Merk op,** in dit voorbeeld interactiemodel doet een datadienstgebruiker een abonnement verzoek bij een datadienstaanbieder. Een abonnement verzoek en abonnement response kan in het DSGO door iedere rol verstuurd worden afhankelijk van de situatie. Bijvoorbeeld een datadienstaanbieder die een abonnement verzoek verstuurt naar een marktvoorziening.




Generiek interactie patroon voor het abonneren op gebeurtenissen van een datadienstaanbieder en notificaties ontvangen

| # | Acties | Omschrijving |
|---|---|---|
| 1 | Abonneren verzoek | De datadienstgebruiker initieert het abonneren op een gebeurtenis door middel van een abonnement verzoek naar de datadienstaanbieder. Hierbij |

| | | |
|---|---|---|
| | | moet de datadienstgebruiker voldoen aan alle voorwaarde van het abonnement zoals gedefinieerd door de datadienstaanbieder. |
| 2 | Abonneren response | De datadienstaanbieder valideert het abonnement verzoek tegen de voorwaarde (zoals gedefinieerd door de datadienstaanbieder, b.v. kosten van het abonneren) van het abonnement en stuurt een geschikte response naar de datadienstgebruiker. |
| 3 | Gebeurtenis | De datadienstaanbieder monitort de resource voor gebeurtenissen zoals beschreven in de abonnementsvoorwaarde. |
| 4 | Notificatie | De datadienstaanbieder stuurt de datadienstgebruiker een notificatie wanneer een gebeurtenis plaatsvindt. |

Wanneer een partij een notificatie ontvangt van een wijziging waarop de partij een abonnement heeft kan de partij er voor kiezen om in actie te komen (zoals het ophalen van aangepaste data) of niet.

De DSGO API's voor het abonneren op een datadienst, het beheren van een abonnement en het ontvangen van notificaties worden hier verder gedetailleerd.

# Datadienst ontdekking

Als een datadienstgebruiker gebruik wil maken van een datadienst van een specifieke datadienstaanbieder, moet deze eerst weten uit welke elementen de datadienst bestaat en wat de specifieke eigenschappen van de datadienst zijn (zie datadienstdefinitie). Pas wanneer de datadienstgebruiker alle nodige informatie over een datadienst kent, kan deze de datadienst gebruiken. In de onderstaande tabel worden de generieke acties die plaatsvinden bij het ontdekken van een datadienst weergegeven. Bij het ontdekken van een datadienst speelt de stelselcatalogus die alle nodige datadienst informatie bevat (b.v deelnemers, datadiensten, dienstvoorwaarden, endpoints etc.) een essentiële rol.

⭐ **Voorbeeld**: De catalogus van het Nationaal Georegister is een voorbeeld van een human-readable stelselcatalogus

| # | Acties | Omschrijving |
|---|---|---|
| 1 | Datadienst-registratie | De datadienstaanbieder definieert zijn geïmplementeerde datadienst in een stelselcatalogus. |
| 2 | Ontdekking-verzoek | De datadienstgebruiker ondervraagt het stelselcatalogus voor informatie over de beschikbare datadiensten. |
| 3 | Ontdekkings-response | Het stelselcatalogus beantwoordt de vraag van de datadienstgebruiker met relevante informatie over de beschikbare datadiensten. |
| 4 | Datadienst-wijziging | De datadienstaanbieder kan zijn geïmplementeerde datadienst wijzigen en moet de definitie in het stelselcatalogus wijzigen zodat dit actueel blijft. |

ℹ In de huidige versie van het afsprakenstelsel dient deze pagina als introductie over afspraken die over het ontdekken van datadiensten gemaakt zullen worden. In een toekomstige versie van het afsprakenstelsel zal dit onderwerp verder worden gedetailleerd.

# Identificatie, Authenticatie en Autorisatie

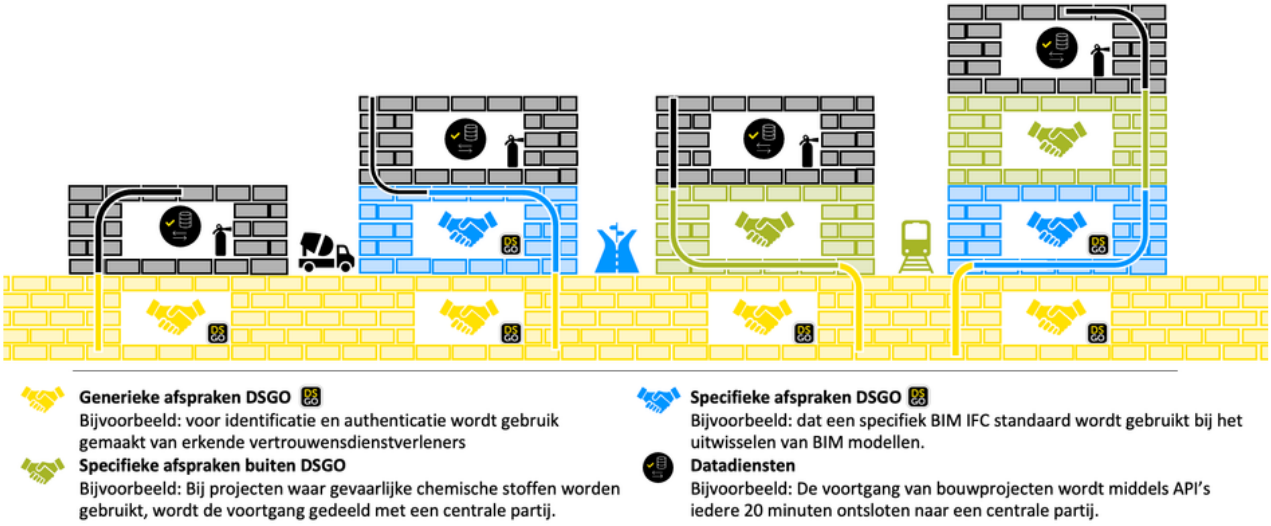
Binnen het afsprakenstelsel wordt ‘Identity en Access Management’ (IAM) gesplitst in de onderwerpen Identificatie, authenticatie en autorisatie. Dit zijn essentiële ondersteunende functionaliteiten die nodig zijn om een datadienst tussen partijen (datadienstaanbieder en -gebruiker) vertrouwd, gecontroleerd mogelijk te maken om data delen op schaal te faciliteren. In de onderstaande tabel worden deze begrippen geïntroduceerd:

| Begrip | Omschrijving |
|---|---|
| Identificatie | Identificatie is het proces waarbij een identiteit wordt toegekend aan of wordt geclaimd door een partij die een rol vervuld in het afsprakenstelsel. Een identiteit wordt uitgedrukt in een identificerend kenmerk zoals bijvoorbeeld naam, e-mailadres, telefoonnummer, KvK nummer, EORI nummer of GS1 GTIN en GLN |
| Authenticatie | Het proces waarbij de geldigheid van een geclaimde identiteit van een partij geverifieerd wordt. Afhankelijk van het nodige betrouwbaarheidsniveau (level of assurance) in de geclaimde identiteit zijn er verschillende manieren om de identiteit te valideren, zoals bijvoorbeeld door middel van een gebruikersnaam & wachtwoord, 2-factor authenticatie of een elektronische handtekening. |
| Autorisatie | Het hebben van rechten of toestemming en het proces waarbij een partij rechten of toestemming krijgt om een specifieke actie uit te voeren. De autorisatie is afhankelijk van de maten van zekerheid (authenticiteit) van het subject. Autorisaties kunnen breed (bedrijf X mag namens bedrijf Y handelen) of fijnmazig (persoon X uit bedrijf Y mag data attribuut Z aanvragen) zijn. Er zijn veel variaties mogelijk in autorisatie zoals bijvoorbeeld het moment (vooraf of ad hoc) en de plaats waar de autorisatie opgeslagen is. |

Om datadiensten op basis van het DSGO mogelijk te maken, zijn er generieke afspraken over identificatie, authenticatie en autorisatie gemaakt.

# Specifieke functionaliteiten

Voor sommige oplossingen zullen specifieke functionaliteiten nodig zijn waarvoor use case-, keten- of branche specifieke afspraken nodig zijn die bovenop de generieke afspraken in het afsprakenstelsel worden gemaakt, zie figuur hieronder.




Het afsprakenstelsel legt de fundering met generieke afspraken waarop, mogelijk met additionele specifieke afspraken, data diensten worden gerealiseerd

Over de volgende onderwerpen zijn specifieke afspraken opgesteld:

- BIM in datadiensten

Op dit moment is het afsprakenstelsel in ontwikkeling binnen het DSGO-programma. In een toekomstige versie van het afsprakenstelsel zal dit hoofdstuk worden doorontwikkeld.

# Juridische bepalingen

Om de schaalbaarheid en betrouwbaarheid van het DSGO te ondersteunen bevat het DSGO een juridische basis. De juridische basis van het DSGO wordt gevormd door de deelnameovereenkomst, de gebruiksvoorwaarden en licenties. Deze juridische documenten bevatten onder andere de rechten en plichten van de verschillende rollen gedefinieerd in het afsprakenstelsel. De juridische documenten zijn zo opgebouwd dat ook niet direct betrokken partijen die wel een belang hebben een partij kunnen aanspreken op de naleving van de toepasselijke rechten en plichten (derdewerking).

## De deelnameovereenkomst

De deelnameovereenkomst is de overeenkomst tussen de beheerorganisatie DSGO en een partij die voornemens is om de rol van datadienstaanbieder of marktvoorziening binnen het DSGO te vervullen. Middels de deelnameovereenkomst wordt het afsprakenstelsel van toepassing verklaard waarmee een partij zich committeert aan de rechten en plichten die voor de te vervullen rol zijn opgesteld. Met het tekenen van een deelnameovereenkomst gedurende het toetredingsproces wordt een partij deelnemer van het DSGO.

De model deelnameovereenkomst van het DSGO is hier beschikbaar.

## De gebruiksvoorwaarden

De gebruiksvoorwaarden zijn opgesteld voor partijen die geen deelnemer zijn van het DSGO (rechthebbende & datadienstgebruiker). Deze partijen ondertekenen geen deelnameovereenkomst en zijn daarom niet direct gebonden aan het afsprakenstelsel. Wanneer deze partijen betrokken zijn bij een datadienst zullen de gebruiksvoorwaarden van toepassing worden verklaard bij een overeenkomst tussen hen en de deelnemer (datadienstaanbieder of marktvoorziening). Met het accepteren van de gebruiksvoorwaarden committeren deze partijen zich aan de rechten en plichten voor de rol die ze vervullen zonder dat ze deelnemer hoeven te worden.

De gebruiksvoorwaarde van het DSGO zijn hier beschikbaar.

## Licenties

Een licentie(overeenkomst) is een juridisch bepaling in de datadienstdefinitie met instructies over welke rechten een datadienstgebruiker toekomen over een aangeboden datadienst (bijv. data lezen niet bewerken, alleen delen met niet commerciële partijen etc.). Licenties zijn een onderdeel van de datadienstdefinitie en wordt aan verwezen. Deze verwijzing refereert aan een uitputtende lijst van licenties met verschillende (gebruiks)rechten die is opgenomen in het afsprakenstelsel. De datadienstgebruiker gaat akkoord met de licentie door akkoord te gaan met de voorwaarde bij een datadienst. De datadienstgebruiker weet daardoor voordat een datadienst wordt uitgevoerd welke licentie van toepassing is op de datadienst.

**Merk op,** de lijst van licenties onder het DSGO is nog in ontwikkeling en zal in een volgende versie van het afsprakenstelsel worden gepubliceerd.

# Governance

Deze pagina beschrijft de governance van het DSGO. Borging van de continuïteit van DSGO vereist een beheerorganisatie die verantwoordelijk is voor doorontwikkeling, adoptie & beheer. Na afloop van het programma DSGO in juni 2024 is beheer, adoptie & doorontwikkeling overgedragen aan de beheerorganisatie DSGO.

**Merk op,** deze governance wordt n.a.v. ontwikkeling en gebruik van het DSGO op termijn mogelijkerwijs aangepast of uitgebreid.

## Uitgangspunten

Op basis van analyse uit andere contexten & interviews zijn een aantal cruciale uitgangspunten voor de governance van het DSGO geïdentificeerd:

- Er wordt zoveel mogelijk gebruik gemaakt van bestaande structuren/beheerprocessen in de sector voor efficiëntie.
- Beheer, adoptie en doorontwikkeling wordt zoveel mogelijk belegd bij één beheerorganisatie DSGO voor efficiëntie.
- Inspraak van de gebruikers van het DSGO dient goed georganiseerd te zijn voor voldoende draagvlak en acceptatie in de sector.
- De gebruiker van het DSGO staat centraal voor afweging van belangen en gedragen keuzes t.a.v. beheer, adoptie & doorontwikkeling. De uitvoerende beheerorganisatie DSGO heeft hierin een faciliterende/ondersteunende rol en blijft te allen tijde onafhankelijk (heeft geen direct belang).

## Activiteiten

### Beheer

Het beheer van het DSGO gaat over het beheren van het federatieve ecosysteem DSGO, inclusief het afsprakenstelsel en voorzieningen. Voor het beheer van het DSGO kunnen de volgende operationele processen worden onderscheiden:

1. Toezicht en handhaving
2. Change en release management
3. Toetreding tot het DSGO, inclusief administratie van deelnemers
4. Uittreding van deelnemers
5. Beheren van stelselvoorzieningen
6. Operationeel support leveren in het DSGO

### Adoptie

Adoptie beslaat de activiteiten die worden uitgevoerd om het gebruik van het DSGO in de gebouwde omgeving te stimuleren. In de fase na afloop van het programma DSGO is waarschijnlijk intensieve ondersteuning voor adoptie nodig. Na verloop van tijd wordt adoptie steeds meer vraaggestuurd ingericht en neemt de behoefte vanuit de sector voor intensieve ondersteuning af.

Adoptie bestaat uit de ondersteuning van potentiële datadienstaanbieders & datadienstgebruikers en het realiseren van bekendheid over het DSGO.

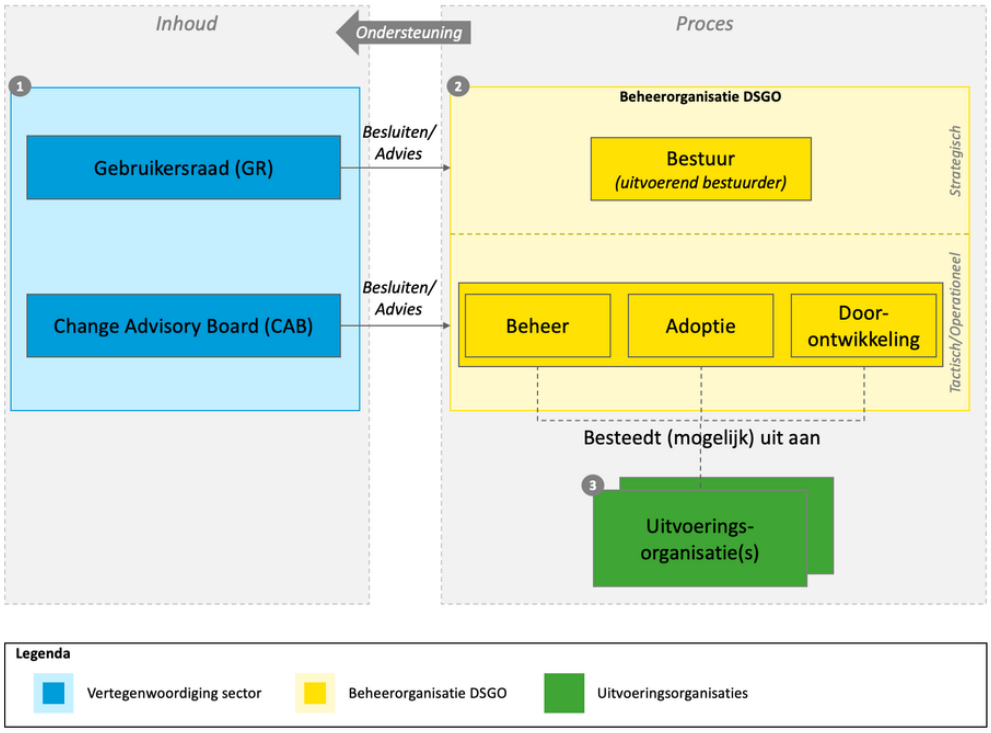
### Doorontwikkeling

In de fase na het programma DSGO is doorontwikkeling van het afsprakenstelsel nodig om een steeds bredere set van use cases te kunnen ondersteunen. Dit bevat onder andere het uitbreiden van functionaliteit van het DSGO middels de doorontwikkeling van het

afsprakenstelsel en het komen tot (met name) specifieke afspraken. Daarnaast is doorontwikkeling en operationaliseren van stelselvoorzieningen in eerste termijn gewenst.

## Governance

In de onderstaande figuur wordt een overzicht gegeven van de governance van het DSGO.



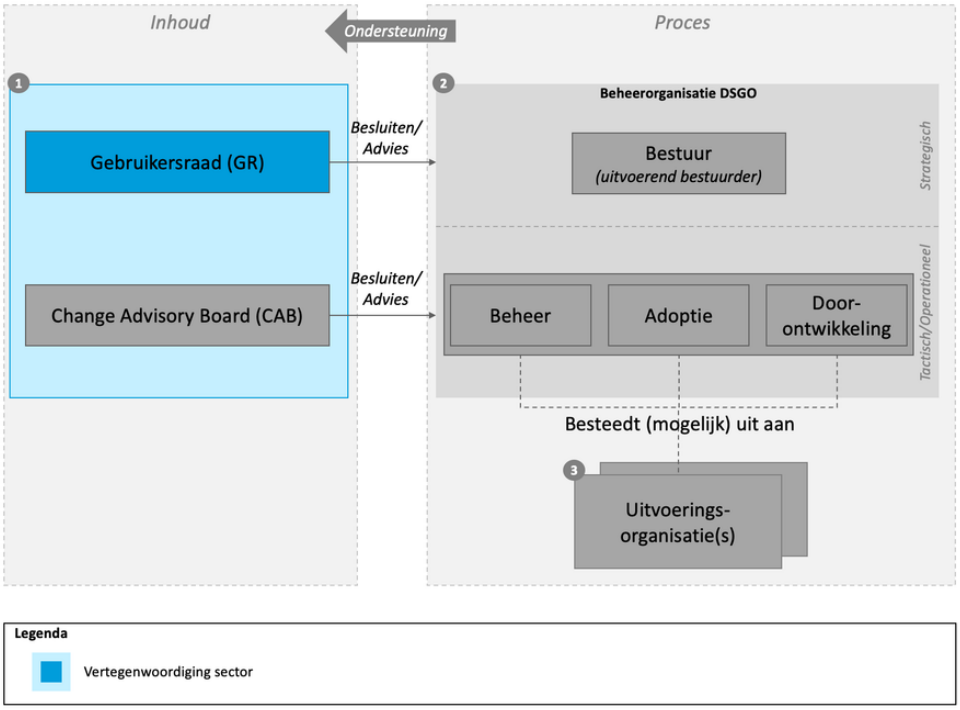

De governance van het DSGO bestaat uit vertegenwoordiging van de sector, de beheerorganisatie DSGO en uitbesteding aan uitvoeringsorganisaties

De governance van het DSGO bestaat uit:

1. Vertegenwoordiging van en besluitvorming door sector & deelnemers DSGO middels een Gebruikersraad (GR) en een Change Advisory Board (CAB). In deze gremia wordt de inhoud voor het DSGO bepaald.
2. Beheerorganisatie DSGO waarin ondersteunende/faciliterende activiteiten worden uitgevoerd onder regie van één of twee uitvoerend bestuurders. In dit deel van de governance worden de activiteiten voor beheer, adoptie & doorontwikkeling uitgevoerd (proces).
3. Eén of meerdere uitvoeringsorganisaties die kunnen worden ingehuurd voor o.a. uitvoeren van activiteiten of het leveren van expertise. Door synergieën te zoeken met andere beheerorganisaties in de sector ontstaat efficiëntie in het uitvoeren van activiteiten. Voor efficiëntie heeft het in het begin de voorkeur om personeel te detacheren of onderdeel te maken van de uitvoerende onderdelen van de beheerorganisatie DSGO (conform het programma DSGO).

# Gebruikersraad

De gebruikersraad borgt betrokkenheid van deelnemers op strategisch niveau door inhoudelijke besluiten over beheer, adoptie & doorontwikkeling van het DSGO.




## Taken/verantwoordelijkheden

- De gebruikersraad neemt inhoudelijke besluiten over beheer, adoptie & doorontwikkeling van het DSGO op basis van eigen belangen/benodigdheden en de richtinggevende principes.
- De gebruikersraad geeft inbreng op de roadmap voor de ontwikkeling van het DSGO.
- De gebruikersraad vraagt aandacht voor relevante problemen of thema's in relatie tot het DSGO.

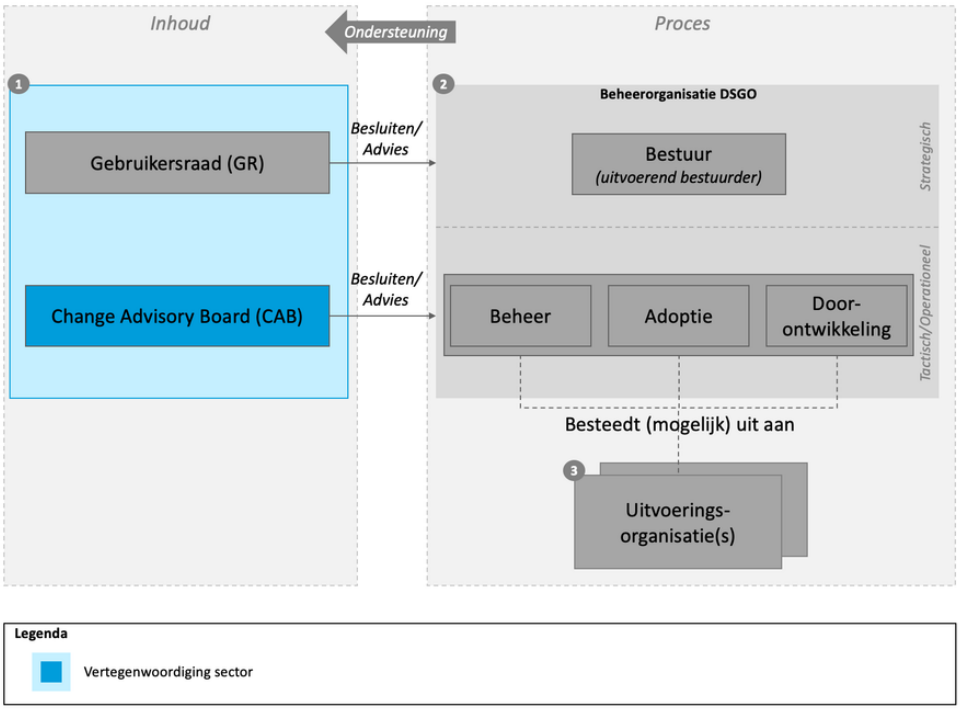
## Samenstelling

- De gebruikersraad bestaat uit deelnemers aan het DSGO. Deelnemers aan het DSGO hebben een deelnameovereenkomst gesloten met de beheerorganisatie en committeren zich daarmee aan het afsprakenstelsel. Deelnemers zijn tenminste alle datadienstaanbieders en marktvoorzieningen.
- Vertegenwoordiging namens deelnemers in de Gebruikersraad is mogelijk.
- Er wordt een onafhankelijke voorzitter aangesteld.
- De Bouw Digitaliseringsraad keurt de samenstelling van de Gebruikersraad goed.
- Indien de beheerorganisatie DSGO afwijkt van de adviezen van de Gebruikersraad, heeft het bestuur van de beheerorganisatie een motiveringsplicht.

**Merk op,** de gebruikersraad kan in het begin worden aangevuld met personen die deelnemer willen worden (boegbeelden). Op termijn krijgt de samenstelling van de Gebruikersraad een meer formeel karakter en wordt de samenstelling geformaliseerd met vastgestelde criteria.

# Change Advisory Board

De Change Advisory Board (CAB) adviseert over het aanpassen en uitbreiden van het DSGO en keuzes omtrent beheer & adoptie.




## Taken & verantwoordelijkheden

De CAB heeft als doel om aansluiting van het DSGO met de ontwikkelingen en wensen van de deelnemers te borgen.

- De CAB adviseert over het aanpassen en uitbreiden van het DSGO binnen de gestandaardiseerde change en release management processen. Daarnaast kan de CAB verzoeken tot wijziging indienen en prioriteren.
- De CAB adviseert over keuzes omtrent beheer en adoptie van het DSGO.
- De CAB borgt de aansluiting van het DSGO bij de wensen en ontwikkelingen in de ontwerp-, bouw- & techniekSector.

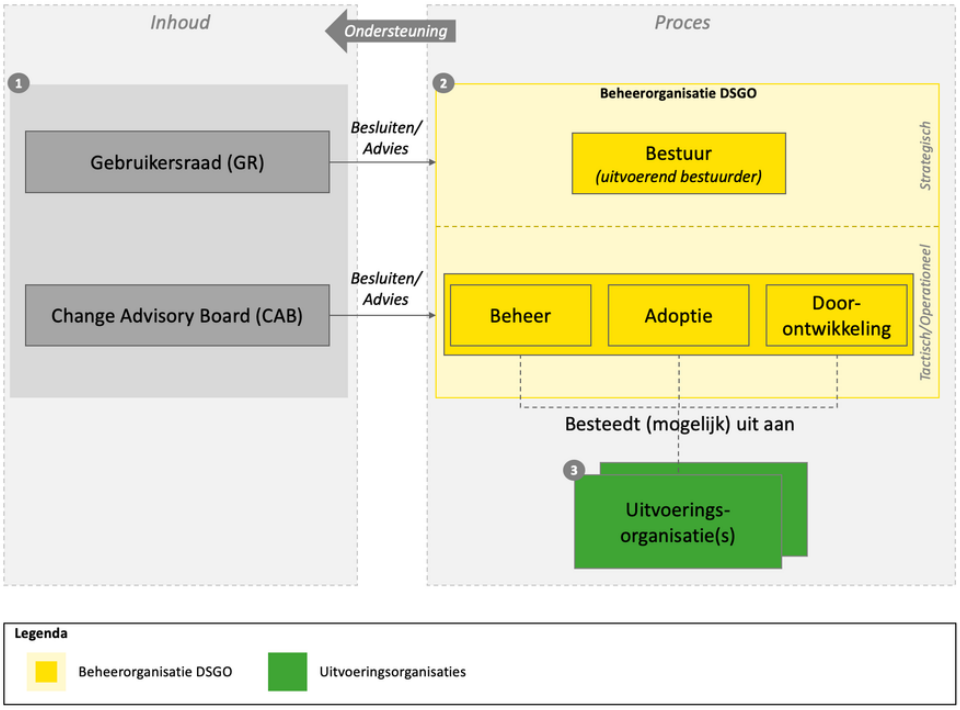
## Samenstelling

- De CAB bestaat uit deelnemers aan het DSGO.
- De CAB wordt benoemd door de Gebruiksraad.
- De samenstelling van de CAB kan wisselen per onderwerp.

**Merk op,** in het begin kan de CAB worden aangevuld met personen die tijdens programmafase actief zijn bij de functionele, technische en juridische reviews. Op termijn krijgt de samenstelling een meer formeel karakter en wordt de samenstelling geformaliseerd met vastgestelde criteria. Op termijn is ook uitbreiding met een operationeel overleg mogelijk.

# De beheerorganisatie DSGO

Het beheerorganisatie is verantwoordelijk het (laten) uitvoeren van de activiteiten rondom beheer, adoptie en doorontwikkeling van het DSGO.




**Merk op,** de stichting digiGO lijkt in eerste termijn meest logische keuze als beheerorganisatie DSGO – De Bouw Digitaliseringsraad vertegenwoordigt de brede gebouwde omgeving.

- Activiteiten worden 'dicht bij huis' georganiseerd – complexiteit overdracht is beperkt
- Financiering van activiteiten door overheid & sector is haalbaar
- Ervaring met ondersteuning van meer programmatische aanpak voor doorontwikkeling & adoptie
- Activiteiten zijn conform doelen & activiteiten statuten stichting digiGO

Activiteiten t.b.v. beheer, adoptie & doorontwikkeling kan worden uitbesteed door de stichting digiGO aan uitvoeringsorganisaties.

## Taken & verantwoordelijkheden niet-uitvoerende bestuurders

- De niet-uitvoerende bestuurders houden toezicht op de uitvoering van de strategie en geven advies over de realisatie van de doelstellingen van de beheerorganisatie DSGO.
- De niet-uitvoerende bestuurders geven advies over realisatie doelstellingen stichting.
- De niet-uitvoerende bestuurders controleren de financiële verslaglegging.
- De niet-uitvoerende bestuurders houden toezicht op de naleving van wet- & regelgeving.
- De niet-uitvoerende bestuurders adviseren over doelmatigheid, kwaliteit & efficiëntie.
- De niet-uitvoerende bestuurders stellen de uitvoerende bestuurders aan en adviseren deze.

In de praktijk wordt vaak een jaarplan gebruikt voor de opdrachtformulering. Via rapportages wordt verantwoording afgelegd door de uitvoerende bestuurder(s).

# Taken & verantwoordelijkheden uitvoerende bestuurder(s)

Het bestuur is verantwoordelijk voor het uitvoeren van de activiteiten met als doel om de continuïteit van DSGO te borgen. De beheerorganisatie DSGO is verantwoordelijk voor de uitvoering van de inhoudelijke activiteiten en ondersteunt de bestuurlijke besluitvorming zoals bepaald door de niet-uitvoerende bestuurders en de Gebruikersraad.

- De uitvoerende bestuurder(s) zijn verantwoordelijk voor het organiseren, managen en uitvoeren van activiteiten in het kader van beheer, adoptie & doorontwikkeling en de regie op de financiën van het DSGO.
- De uitvoerende bestuurder(s) creëert/creëren de condities voor effectief en efficiënt beheer, adoptie & doorontwikkeling.
- De uitvoerende bestuurder(s) wijst/wijzen duidelijke verantwoordelijkheden binnen de beheerorganisatie DSGO toe en bepaald/bepalen welke activiteiten worden uitgevoerd door uitvoeringsorganisaties.
- De uitvoerende bestuurder(s) legt rapportage en verantwoording af aan de niet-uitvoerende bestuurders en de Gebruikersraad.

# Generieke afspraken

In de introductie zijn de aanleiding, het doel van het DSGO, en de richtinggevende principes van het afsprakenstelsel gepresenteerd. In de kern van het afsprakenstelsel zijn datadiensten, het rollenmodel en de ondersteunende functionaliteiten die deel uitmaken van het DSGO geïntroduceerd. In dit hoofdstuk worden alle generieke afspraken die nodig zijn om de voorwaarden te scheppen om het aanbieden, vinden en gebruiken van datadiensten schaalbaar, interoperabel en betrouwbaar te faciliteren gepresenteerd.

Het BLOFT-raamwerk bevat een uitgebreide lijst van onderwerpen die het startpunt vormen voor het maken van afspraken binnen het afsprakenstelsel.

- Generieke technische standaarden
- API specifications
- Identificatie
- Authenticatie
- Autorisatie
- Informatiebeveiliging
- Juridische context
- Service level agreements
- Operationele processen
- Marktvoorzieningen
- Stelselvoorzieningen

# Generieke technische standaarden

In het algemeen volgt het afsprakenstelsel technische open standaarden. Hiermee is het afsprakenstelsel in lijn met de API strategie voor de Nederlandse Overheid, het iSHARE scheme en het Data Sharing Coalition Use Case Implementation Guide die gebaseerd zijn op deze zelfde standaarden. In het afsprakenstelsel worden API's (Application Programming Interfaces) gedefinieerd om communicatie en data delen tussen partijen mogelijk te maken. De gespecificeerde API's maken gestandaardiseerde interactie tussen de systemen van verschillende partijen mogelijk. In de onderstaande tabel worden de gebruikte generieke standaarden geïntroduceerd.

| Standaard | Beschrijving | Link |
|---|---|---|
| APIs | Een Application Programming Interface (API) is een set van definities en protocollen waarmee verschillende softwareapplicaties met elkaar kunnen communiceren. Het stelt ontwikkelaars in staat om functionaliteiten van een externe applicatie te gebruiken. | RESTful API's |
| RESTful | RESTful principes zijn ontwerpprincipes voor het ontwikkelen van API's. Bij het gebruik van RESTful API's is het van belang dat logische resources gescheiden zijn. Resources kunnen worden gemanipuleerd met HTTP-operaties. | RESTful API's |
| HTTP(s) | HyperText Transfer Protocol (HTTP) is een open standaard voor een communicatieprotocol tussen webclients en webservers. HTTPS is een beveiligde versie van HTTP die gebruik maakt van encryptie om de communicatie tussen de client en de server te beveiligen. | HTTP(s) |
| TLS | Transport Layer Security (TLS) is een open standaard voor de encryptie van communicatie tussen webclients en webservers. Het wordt gebruikt voor het zorgen voor vertrouwelijkheid en integriteit van alle communicatie. | Transport layer security |
| PKI | Public Key Infrastructure (PKI) is een systeem van processen en technologieën voor het beveiligen van communicatie met behulp van openbare en privésleutels. Het stelt gebruikers in staat om digitale certificaten te verkrijgen en te beheren om hun identiteit te verifiëren en beveiligde communicatie te garanderen. | Ondertekening |
| OAuth 2.0 | OAuth 2.0 is een open standaard protocol voor autorisatie van toegang tot applicaties en diensten op het internet. Het stelt gebruikers in staat om veilig toegang te geven tot hun data op een andere applicatie of dienst. | Autorisatie |
| JSON | JavaScript Object Notation (JSON) is een open standaard data format die niet afhankelijk is van een specifieke programmeertaal. Dit compacte dataformaat maakt gebruik van gemakkelijk te lezen tekst om dataobjecten uit te wisselen tussen toepassingen en voor dataopslag. In het afsprakenstelsel wordt JSON wordt voor het sturen van gegevens in de context van datadiensten. Dit geldt niet voor de inhoud van de data die wordt uitgewisseld, het DSGO is data agnostisch en ondersteund hiervoor alle mogelijke data soorten. | JSON |
| JWT | Een JSON Web Token (JWT) is een open standaard voor een compacte token die wordt gebruikt voor authenticatie en autorisatie. Het kan worden gebruikt om veilig data over te dragen tussen partijen en om te controleren of de data niet zijn gewijzigd tijdens de overdracht. | JSON Web Tokens (JWT) |
| UTC | Coordinated Universal Time (UTC) is de standaardtijd die wereldwijd wordt gebruikt als referentie voor tijd. | UTC |

# RESTful API's

Het afsprakenstelsel maakt gebruik van RESTful API's. Hiermee is het afsprakenstelsel in lijn met de API strategie voor de Nederlandse Overheid, het iSHARE scheme en het Data Sharing Coalition Use Case Implementation Guide die gebaseerd zijn op deze zelfde principes.

Wanneer een specifieke datadienst een specifieke reden heeft om af te wijken van een RESTful-implementatie om hun datadienst mogelijk te maken (bv. wegens legacy-beperkingen), is dit mogelijk. Daarom is deze eis een zou.

✔️ Partijen ZOUDEN RESTful architectuurprincipes MOETEN volgen voor API's

## Introductie API's

:Quotes:

**Bron:** API strategie voor de Nederlandse Overheid - 2.3 Wat is een API

Een Application Programming Interface (API) is een combinatie van technische bestanden, documentatie en andere ondersteuning die helpen bij het aanroepen van externe applicaties (Als het in deze API-strategie gaat over API's dan bedoelen we daarmee RESTful API's). Een API wordt gepubliceerd door een softwareontwikkelaar, zodat andere ontwikkelaars weten hoe de software te koppelen aan de eigen software. Zodoende kunnen twee applicaties rechtstreeks en online met elkaar communiceren. Het is daarmee geen standaard, maar eerder een handleiding die kan worden gebruikt voor een machine tot machine koppeling. Met name daar waar veel digitale diensten met elkaar samenwerken en informatie realtime op een makkelijke en toegankelijke manier willen delen zijn API's zeer geschikt. De belangrijke eigenschappen van moderne API's zijn:

- prestaties (het zorgt ervoor dat machines snel met elkaar praten);
- schaalbaarheid (het zorgt ervoor dat het blijft werken bij veel gebruik(ers);
- simpele interfaces (de communicatie tussen componenten is eenvoudig en overzichtelijk).

*API's kunnen gezien worden als 'proven technology', er is veel kennis over en ervaring mee in de markt. Berichten uitwisselen via API's is niet perse onveiliger of veiliger dan hoe de overheid op dit moment haar berichtenuitwisseling organiseert. Het gebruik van API's beperkt zich daarmee niet alleen tot open data, maar kan juist ook goed worden ingezet voor meer gevoelige / gesloten data.*

## RESTful principes

Bij het gebruik van RESTful API's is het van belang dat logische resources gescheiden zijn. Resources kunnen worden gemanipuleerd (middels een datadienst) met HTTP-operaties.

:Quotes:

**Bron:** API strategie voor de Nederlandse Overheid - 4.2 RESTful principes

Het belangrijkste principe van REST is het scheiden van de API in logische resources ("dingen"). De resources beschrijven de informatie van het "ding". Deze resources worden gemanipuleerd met behulp van HTTP-verzoeken en HTTP-operaties. Elke operatie (`GET`, `POST`, `PUT`, `PATCH`, `DELETE`) heeft een specifieke betekenis, zie onderstaande tabel.

HTTP definieert ook operaties als `HEAD`, `TRACE`, `OPTIONS` en `CONNECT`. Deze worden echter in de context van REST vrijwel niet gebruikt en zijn daarom in de verdere uitwerking weggelaten.

| Operatie | CRUD | Toelichting |
|---|---|---|
| `POST` | Create | Wordt gebruikt als een "create" voor resources (ofwel `POST` voegt een resource toe aan de collectie). |

| | | |
|---|---|---|
| `GET` | Read | Wordt gebruikt om een resource op te vragen van de server. Data wordt alleen opgevraagd en niet gewijzigd. |
| `PUT` | Update | Wordt gebruikt om een specifieke resource te vervangen. Is óók een "create" wanneer de resource op aangegeven identifier/URI nog niet bestaat. |
| `PATCH` | Update | Wordt gebruikt om een bestaande resource gedeeltelijk bij te werken. Het verzoek bevat de gegevens die gewijzigd moeten worden en de operaties die de resource muteren in het daarvoor bedoelde JSON merge patch formaat (RFC 7386). |
| `DELETE` | Delete | Verwijdert een specifieke resource. |

✔️ Partijen MOETEN uitsluitend standaard HTTP-operaties ondersteunen (GET, PUT, POST, PATCH, DELETE)

✔️ Partijen MOGEN NIET de state van de client bij houden

## Resources

Binnen het Afsprakenstelsel wordt data als resources beschikbaar gesteld.

✔️ Partijen MOETEN data als resources beschikbaar stellen in een datadienst

✔️ Partijen MOETEN resources een zelfstandig naamwoord in het meervoud als naam geven

:Quotes:

**Bron:** API strategie voor de Nederlandse Overheid - 4.2.1 Wat zijn resources?

Het fundamenteel concept in elke RESTful API is de resource. Een resource is een object met een type, bijbehorende data, relaties met andere resources en een aantal operaties om deze te bewerken. Resources worden aangeduid met zelfstandige naamwoorden (niet werkwoorden!) die relevant zijn vanuit het perspectief van de afnemer van de API. Dus resources zijn zelfstandige naamwoorden en operaties zijn werkwoorden. Operaties zijn acties die op resources worden uitgevoerd.

Het is mogelijk om interne datamodellen één-op-één toe te wijzen aan resources, maar dit hoeft niet per definitie zo te zijn. De crux is om alle niet relevante implementatiedetails te verbergen. Enkele voorbeelden van resources zijn: aanvraag, activiteit, pand, rijksmonument en vergunning.

Als de resources geïdentificeerd zijn, wordt bepaald welke operaties van toepassing zijn en hoe deze worden ondersteund door de API. RESTful API's realiseren CRUD (Create, Read, Update, Delete) operaties met behulp van HTTP-operaties, zie tabel hieronder.

Het mooie van REST is dat er gebruik wordt gemaakt van de bestaande HTTP-operaties om de functionaliteit te implementeren met één enkel eindpunt. Hierdoor zijn er geen aanvullende naamgevingsconventies nodig in de URI en blijft de URIstructuur eenvoudig.

| Request | Omschrijving |
|---|---|
| `GET /aanvragen` | Haalt een lijst van aanvragen op |
| `GET /aanvragen/12` | Haalt aanvraag #12 op |
| `POST /aanvragen` | Creëert een nieuwe aanvraag |
| `PUT /aanvragen/12` | Wijzigt aanvraag #12 als geheel |
| `PATCH /aanvragen/12` | Wijzigt een gedeelte van aanvraag #12 |
| `DELETE /aanvragen/12` | Verwijdert aanvraag #12 |

# HTTP(s)

Het afsprakenstelsel maakt gebruik van HTTP(s) communicatie, beveiligd met TLS. HyperText Transfer Protocol (HTTP) is een communicatieprotocol voor internet en andere computernetwerken. Hiermee is het afsprakenstelsel in lijn met de API strategie voor de Nederlandse Overheid, het iSHARE scheme en het Data Sharing Coalition Use Case Implementation Guide die gebaseerd zijn op deze zelfde standaarden.

✔️ Partijen MOETEN in de context van datadiensten communiceren via het HTTP procotol

In het hoofdstuk informatiebeveiliging staan op de pagina's Transport Layer Security en Public Key Infrastructure (PKI) en X.509 gedetailleerdere eisen voor de toepassing van TLS om communicatie via het HTTP te beveiligen.

## HTTP Headers

Omdat in het afsprakenstelsel data over identificatie, authenticatie en autorisatie verzonden wordt in HTTP headers, moeten grote HTTP headers worden geaccepteerd, in lijn met iSHARE.

:Quotes:

**Bron:** iSHARE - HTTP(s)

iSHARE authentication/authorization data is generally transferred in HTTP Headers. These headers can become very large when containing multiple encrypted certificates or JWT's. iSHARE parties SHOULD configure their web servers to accept HTTP headers of 100K length to minimise implementation impact on current services.

✔️ Partijen MOETEN HTTP-headers van 100K lengte accepteren

## HTTP Status codes

HTTP definieert standaard statuscodes die gebruikt moeten worden bij het antwoorden op een API verzoek. Deze worden beschreven in onderstaande tabel:

| HTTP statuscode | Toelichting |
|---|---|
| `200 OK` | Reactie op een succesvolle `GET`, `PUT`, patch of `DELETE`. Ook geschikt voor `POST` die niet resulteert in een creatie |
| `201 Created` | Reactie op een `POST` die resulteert in een creatie. Moet worden gecombineerd met een locatie-header die wijst naar de locatie van de nieuwe resource |
| `204 No Content` | Reactie op een succesvol verzoek die geen inhoud zal teruggeven (zoals een `DELETE`) |
| `304 Not Modified` | Gebruikt wanneer HTTP caching headers worden toegepast |
| `400 Bad Request` | Het verzoek is onjuist, bijvoorbeeld als het verzoek (body) niet kan worden geïnterpreteerd |
| `401 Unauthorized` | Als er geen of ongeldige authenticatie details worden verstrekt. Ook handig om een authenticatie-venster te tonen als de API wordt gebruikt vanuit een browser |
| `403 Forbidden` | Als de authenticatie gelukt is maar de geverifieerde gebruiker geen toegangsrechten heeft voor de resource |

| | |
|---|---|
| `404 Not Found` | Wanneer een niet-bestaande resource is opgevraagd |
| `405 Method Not Allowed` | Wanneer een HTTP-methode wordt gebruikt die niet is toegestaan voor de geauthentiseerde gebruiker |
| `406 Not Acceptable` | Wordt teruggegeven als het gevraagde formaat niet ondersteund wordt (onderdeel van content negotiation) |
| `409 Conflict` | Het verzoek kon ik niet worden verwerkt als het gevolg van een conflict met de huidige toestand van de resource |
| `410 Gone` | Geeft aan dat de resource niet langer op het eindpunt beschikbaar is. Nuttig als een overkoepelend antwoord voor oude API versies |
| `412 Precondition Failed` | De preconditie die wordt gegeven door één of meer velden in de request-header, ontbraken of zijn na validatie op de server afgekeurd |
| `415 Unsupported Media Type` | Als een verkeerd content-type als onderdeel van het verzoek werd meegegeven |
| `422 Unprocessable Entity` | Gebruikt voor een verzoek (body) dat correct is maar dat de server niet kan verwerken |
| `429 Too Many Requests` | Wanneer een aanvraag wordt afgewezen als het aantal verzoeken per tijdsperiode is overschreden |
| `500 Internal Server Error` | Wanneer een onverwachte fout optreedt en het beantwoorden van het verzoek wordt verhinderd |
| `503 Service Unavailable` | Wordt gebruikt als de API niet beschikbaar is (bijv. door gepland onderhoud) |

:Quotes:

**Bron:** API strategie voor de Nederlandse Overheid - HTTP statuscodes

HTTP definieert een hele reeks gestandaardiseerde statuscodes die gebruikt dienen te worden door API's. Deze helpen de gebruikers van de API's bij het afhandelen van fouten. Zie tabel hieronder met een samenvatting van HTTP-operaties in combinatie met de primaire HTTP statuscodes. In de tabel daaronder en korte lijst met een beschrijving van de HTTP statuscodes die minimaal worden toegepast:

| Operatie | CRUD | Gehele collectie (bijvoorbeeld /resource) | Specifieke item (bijvoorbeeld `/resource/\<id>`) |
|---|---|---|---|
| `POST` | Create | 201 (Created), HTTP header `Location` met de URI van de nieuwe resource (`/resource/\<id>`) | 405 (Method Not Allowed), 409 (Conflict) als de resource al bestaat |
| `GET` | Read | 200 (OK), lijst van resources. Gebruik pagineren, filteren en sorteren om het werken met grote lijsten te vereenvoudigen | 200 (OK) enkele resource, 404 (Not Found) als ID niet bestaat of ongeldig is |
| `PUT` | Update | 405 (Method Not Allowed), behalve als het de bedoeling is om toe te staan elke resource in een collectie te vervangen | 200 (OK) of 204 (No Content), 404 (Not Found) als ID niet bestaat of ongeldig is |
| `PATCH` | Update | 405 (Method Not Allowed), behalve als het de bedoeling is om toe te staan de gehele collectie te wijzigen. | 200 (OK) of 204 (No Content), 404 (Not Found) als ID niet bestaat of ongeldig is |
| `DELETE` | Delete | 405 (Method Not Allowed), behalve als het de bedoeling is toe te staan de gehele collectie te verwijderen | 200 (OK) of 404 (Not Found) als ID niet bestaat of ongeldig is |

- ✔️ Partijen MOETEN bij het ontvangen van een HTTP-verzoek antwoorden met (onder andere) een statuscode die het resultaat van het verzoek aangeeft
- ✔️ Partijen MOETEN geschikte HTTP-statuscodes ondersteunen die passen bij de dienst. Tenminste de volgende: 2XX, 4XX en 5XX
- ✔️ Partijen ZOUDEN de standaard foutmeldingen van de HTTP 400 en 500 statuscode reeksen MOETEN ondersteunen volgens RFC 9110

# JSON

Het afsprakenstelsel maakt gebruik van JSON format voor de communicatie van gegevens in de context van een datadienst. Hiermee is het afsprakenstelsel in lijn met de API strategie voor de Nederlandse Overheid, het iSHARE scheme en het Data Sharing Coalition Use Case Implementation Guide die gebaseerd zijn op deze standaard.

JSON (JavaScript Object Notation) is een standaard voor de formattering van data. JSON is een open standaard die niet afhankelijk is van een specifieke programmeertaal. Dit compacte dataformaat maakt gebruik van menselijk leesbare tekst om dataobjecten (gestructureerde data) uit te wisselen tussen toepassingen en voor dataopslag. De recentste versie van de JSON-specificatie is te vinden op json.org.

✔️ Partijen MOETEN JSON gebruiken voor het sturen van gegevens in de context van datadiensten

# UTC

Het afsprakenstelsel maakt gebruik van de UTC format voor de communicatie van datums en tijdstippen in de context van een datadienst. Hiermee is het afsprakenstelsel in lijn met de API strategie voor de Nederlandse Overheid, het iSHARE scheme en het Data Sharing Coalition Use Case Implementation Guide die gebaseerd zijn op deze standaard.

Coordinated Universal Time (UTC) is een tijdstandaard gebruikt om de tijd vast te leggen. Overal ter wereld is de tijd volgens UTC hetzelfde. De UNIX-format is een manier om de tijd bij te houden als een lopend totaal van seconden, en is breed gebruikt in de informatica. Het gebruik van de UNIX-format om een UTC-tijdstip uit te drukken wordt door alle servers (computers) eenduidig geïnterpreteerd.

- ✔️ Partijen MOETEN alle datums en tijdstippen vastgelegd in de generieke technische standaarden van het afsprakenstelsel DSGO communiceren in UTC-tijd

- ✔️ Partijen MOETEN alle datums en tijdstippen vastgelegd in de generieke technische standaarden van het afsprakenstelsel DSGO formatteren volgens het UNIX timestamp

# API specifications

*Deze pagina's zijn in het engels ten behoeve van mogelijk internationale ontwikkelaars*

All API endpoints defined in this section follow the generic requirements presented here. In doing so, all these endpoints are in line with the iSHARE scheme, the Data Sharing Coalition Use Case Implementation Guide and the API strategie voor de Nederlandse Overheid.

The endpoints defined are categorised by the roles they are relevant for:

- Generic API requirements
- Common endpoints
- Data service provider endpoints
- Data service consumer endpoints
- Trust framework catalogue endpoints

# Generic API requirements

*Deze pagina's zijn in het engels ten behoeve van mogelijk internationale ontwikkelaars*

This page defines a number of requirements that all trust framework APIs must conform to.

✔️ Parties MUST validate that all received API calls conform to the trust framework API requirements

✔️ Parties MUST validate that all responses to API calls conform to the trust framework API requirements

## Endpoint urls

All URLs of API endpoints within the trust framework should follow the following common structure.

✔️ Parties MUST define the default base URL of API endpoints following the `<domain-name>/<path>/resources` format, where `<domain-name>` is server specific and `<path>` is an optional URL path

✔️ Parties MUST define the default base URL of API endpoints without a trailing slash

## Body content

To ensure that API performance requirements can be met, only limited data should be returned in an API call. Therefore, the size of data sent via APIs is limited. If the party sending the API request requires additional or specific data, this can be requested using optional URL query parameters.

✔️ Parties SHOULD limit API responses to include only a reasonably sized amount of data

✔️ Parties MUST NOT include HTTP bodies in GET or DELETE requests

## Query parameters

URL query parameters may be used to modify API queries. A query option is a set of query string parameters applied to a resource that can help control the amount of data being returned for the resource in the URL. A query option requests that a service perform a set of transformations on its data before returning the results. These transformations include functions such as filtering, sorting, searching etc. Depending on the specific resource, the use of URL parameters may be relevant. The trust framework follows the OData 4.01 query options in the use of URL parameters.

✔️ Parties MAY include query options for functionalities such as filter, sort, and page in their API endpoint as defined in OData 4.01

✔️ Parties MUST reject any requests that contain unsupported url parameters with a `501 Not Implemented` as defined in OData 4.01

# Caching

Often, data is temporarily stored in a place different from the source storage location of the data to allow faster access to the data. This is called caching and is a way to improve efficiency.

:Quotes:

**Source:** iSHARE - Caching

Caching is a way to boost performance efficiency. Often data is temporarily stored on a different medium, to enable faster access to the data.

For every API exposed under iSHARE caching MUST be made explicit to the API consumer.

If a response is not cacheable it MUST contain the following headers:

`Cache-Control: no-store`

`Pragma: no-cache`

If a response is cacheable it MUST contain the following headers:

`Cache-Control: max-age=31536000`

Note: `max-age` MAY vary

The trust framework follows the iSHARE scheme and the Data Sharing Coalition Use Case Implementation Guide in regard to caching.

✔️ Parties MUST make caching explicit to API users

✔️ Parties MUST include the following headers in the API response when it is not cacheable:
`cache-control: no-store`
`pragma: no-cache`

✔️ Parties MUST include the following headers in the API response when it is cacheable:
`cache-control: max-age=31536000`
Note: `max-age` MAY vary

# Common endpoints

*Deze pagina's zijn in het engels ten behoeve van mogelijk internationale ontwikkelaars*

The following API endpoints and requirements are generic and relevant for all parties

- /token
- /capabilities

# /token

*Deze pagina's zijn in het engels ten behoeve van mogelijk internationale ontwikkelaars*

Access tokens are used by parties to as credentials to gain access to a service. For example, this includes data service consumers requiring credentials from a data service provider to access a data service and data service providers requiring credentials from the trust framework catalog to access a market facility. Access tokens can be requested at all partijes via the `/token` endpoint. For detailed information about the use of the `/token` endpoint see Access Token.

✔️ Parties MUST provide an access token via the `/token` endpoint

Due to potential HTTP size restrictions on the server, a POST call to the `/token` endpoint must be provided. Therefore, to avoid unaccepted GET calls, these must be disabled to the `/token` endpoint.

✔️ Parties MUST NOT accept GET calls to the `/token` endpoint

All APIs should follow the generic technical requirements, as well as the requirements specified for specific methods. The specific methods available at an `/token` endpoint are further detailed and specified in the pages below:

- POST /token
- POST /token/revoke

**Visualize OpenAPI (Swagger) documentation app**

Export to PDF of the OpenAPI specification is not supported. See interactive documentation online.

# POST /token

Creates and provides a new access token. This method results in an access token with which the requesting party can gain access to a service at the providing party. The format of an access token is not defined by this specification. They are left to the server and should be opaque to a requesting party.

✔️ Parties MUST support a POST call to a `/token` endpoint to create a new access token

## Prerequisites

In OAuth 2.0 clients are typically “pre-registered” by the server. In the DSGO this is not desirable as data can be shared with previously unknown clients. Therefore client identification and authentication is performed via a check by the Trust Framework Authority via the Trust Framework catalog. For more details see the Access Token flow.

✔️ Parties MUST NOT pre-register clients

## Request

### Headers

✔️ Parties MUST validate that a POST request to a `/token` endpoint contains the HTTP headers as described in the table below

| Header | | Description |
|---|---|---|
| `Content-Type` | Required | as the OAuth 2.0 JWT bearer profile, specified in RFC7523. Defines request body content type. MUST be equal to “`application/x-www-form-urlencoded`" |

### Parameters

For information about the parameters that are common to trust framework’s API’s see Generic API Requirements.

✔️ Parties MUST validate that a POST request to a `/token` endpoint contains the parameters as described in the table below

✔️ Parties MUST validate the client credentials in the `client_assertion` received in a POST to a /token endpoint, by comparing the `client_id` to the `iss` and `sub` claim in the `client_assertion` and the `subject_name` of the QSEAL used to sign the `client_assertion`

| Parameters | | Description |
|---|---|---|
| `grant_type` | Required | as the OAuth 2.0 grant type. MUST be equal to “`client_credentials`" |
| `scope` | Required | as the OAuth 2.0 scope. MUST contain the value “`dsgo ishare`" to indicate usage within the DSGO, in |

| | | |
|---|---|---|
| | | alignment with iSHARE |
| `client_id` | Required | as the OAuth 2.0 JWT bearer profile, specified in RFC7523. MUST contain a valid EORI identifier of the data service consumer. (see Idenificatie van Organisaties). Used in DSGO for client identification |
| `client_assertion_type` | Required | as the OAuth 2.0 JWT bearer profile, specified in RFC7523. MUST be equal to "`urn:ietf:params:oauth:client-assertion-type:jwt-bearer`" |
| `client_assertion` | Required | as the OAuth 2.0 JWT bearer profile, specified in RFC7523. MUST contain a signed DSGO Basic JWT. Used in DSGO for authentication of the client identification. |

Example request body for a POST /token call

```
{
    "grant_type"="client_credentials"&
    "scope"="dsgo"&
    "client_id"="EU.EORI.NL000000001"&
    "client_assertion_type"="urn:ietf:params:oauth:client-assertion-type:jwt-bearer"&
    "client_assertion"="eyJhbGciOiJSUzI1NiIsImtpZCI6IjIyIn0.eyJpc3Mi[...omitted for brevity...].cC4hiUPo[...o
}
```

## Response

For information about the parameters that are common to trust framework's API's see Generic API Requirements.

### 200 OK

When a valid request is sent an OK result should be returned and an access token is sent.

#### Headers

✔️ Parties MUST include the HTTP headers as described in the table below in a response to a POST request to a `/token` endpoint

| Header | | Description |
|---|---|---|
| `content-Type` | Required | Defines response body content type. Must be equal to "`application/json`" |

#### Parameters

✔️ Parties MUST include an access token as described in the table below in the HTTP payload in a response to a successful POST request to a `/token` endpoint

✔️ Parties MUST NOT issue refresh tokens

| Parameters | Description |
|---|---|

| | | |
|---|---|---|
| `access_token` | Required | as the OAuth 2.0 access token. The access token which will be used to access endpoints that require authorization |
| `token_type` | Required | as the OAuth 2.0 JWT bearer profile, specified in RFC7523. MUST be equal to "`bearer`" |
| `expires_in` | Required | Access token expiration time in seconds. SHOULD be "`3600`" |

An example M2M Authorization response (200 OK) is presented below

Example HTTP payload in a response to a success POST to the /token endpoint

```
{
    "access_token":"aW2ys9NGE8RjHPZ4mytQivkWJO5HGQCYJ7VyMNGGDLIOw",
    "token_type":"bearer",
    "expires_in":3600
}
```

## 400 Bad Request

When invalid request is sent a bad request result should be returned.

✔️ Parties MUST include the parameters as described in the table below in the HTTP payload in a response to a failed POST request to a `/token` endpoint

| Parameters | | Description |
|---|---|---|
| `error` | Required | as specified in OAuth 2.0 section 5.2, an error code |
| `error_description` | Optional | as specified in OAuth 2.0 section 5.2, a human-readable text providing additional information |
| `error_uri` | Optional | as specified in OAuth 2.0 section 5.2, a URI identifying a human-readable web page with information about the error |

Example HTTP payload in a response to a failed POST to the /token endpoint

```
{
    "error":"invalid_request"
}
```

# POST /token/revoke

Revokes an access token previously obtained. This method results in the revocation of an access token by a party such that it cannot be used by the requesting party to gain access to a service.

✔️ Parties MUST support a POST call to a `/token/revoke` endpoint to revoke an access token

## Request

### Headers

✔️ Parties MUST validate that a POST request to a `/token/revoke` endpoint contains the HTTP headers as described in the table below

| Header | | Description |
|---|---|---|
| `Content-Type` | Required | as the OAuth 2.0 Token Revocation specified in RFC7009. Defines request body content type. Must be equal to "`application/x-www-form-urlencoded`" |

### Parameters

For information about the parameters that are common to trust framework's API's see Generic API Requirements.

✔️ Parties MUST validate that a POST request to a `/token/revoke` endpoint contains the parameters as described in the table below

✔️ Parties MUST validate the client credentials in the `client_assertion` received in a POST to a /token/revoke endpoint

| Parameters | | Description |
|---|---|---|
| `grant_type` | Required | as the OAuth 2.0 grant type. MUST be equal to "`client_credentials`" |
| `client_id` | Required | as the OAuth 2.0 JWT bearer profile, specified in RFC7523. MUST contain a valid EORI identifier of the data service consumer. (see Identificatie van Organisaties). Used in DSGO for client identification. |
| `client_assertion_type` | Required | as the OAuth 2.0 JWT bearer profile, specified in RFC7523. MUST be equal to "`urn:ietf:params:oauth:client-assertion-type:jwt-bearer`" |
| `client_assertion` | Required | as the OAuth 2.0 JWT bearer profile, specified in RFC7523. MUST contain a signed DSGO Basic JWT. Used in DSGO for authentication of the client identification. |
| `token` | Required | as the OAuth 2.0 access token. MUST be equal to access token that the client wants revoked as specified in RFC7009 |

Example request body for a POST /token/revoke call

```
{
    "grant_type"="client_credentials"
    "client_id"="EU.EORI.NL000000001"&
    "client_assertion_type"="urn:ietf:params:oauth:client-assertion-type:jwt-bearer"&
    "client_assertion"="eyJhbGciOiJSUzI1NiIsImtpZCI6IjIyIn0.eyJpc3Mi[...omitted for brevity...].cC4hiUPo[...o
    "token"="aW2ys9NGE8RjHPZ4mytQivkWJO5HGQCYJ7VyMNGGDLIOw"
}
```

# Response

For information about the parameters that are common to trust framework's API's see Generic API Requirements.

## 200 OK

When the access token is successfully revoked, or an invalid token is submitted, the data service provider should send an OK result.

✔ Parties MUST respond with a `200 OK` to a successful POST call to a `/token/revoke` endpoint

✔ Parties MUST respond with a `200 OK` to a POST call to a `/token/revoke` endpoint containing an invalid access token

✔ Parties MUST no longer accept the revoked the access token after a `200 OK` response is responded

## 400 Bad Request

When invalid request is sent a bad request result should be returned.

✔ Parties MUST include the parameters as described in the table below in the HTTP payload in a response to a failed POST request to a `/token/revoke` endpoint

| Parameters | | Description |
|---|---|---|
| `error` | Required | as specified in OAuth 2.0 section 5.2, an error code |
| `error_description` | Optional | as specified in OAuth 2.0 section 5.2, a human-readable text providing additional information |
| `error_uri` | Optional | as specified in OAuth 2.0 section 5.2, a URI identifying a human-readable web page with information about the error |
| `unsupported_token_type` | Optional | as specified in RFC 7009 section 2.2.1 if the server does not support the revocation of the presented token type. |

Example HTTP payload in a response to a failed POST to the /token/revoke endpoint

```
{
    "error":"invalid_request"
}
```

## 503 Service Unavailable

When a 503 response code is sent the requesting party must assume that the token still exists and may retry after a reasonable delay.

✔️ Parties MAY include a `Retry-After` header in the 503 response to a `/token/revoke` endpoint to indicate the expected unavailability of the service

# /capabilities

*Deze pagina's zijn in het engels ten behoeve van mogelijk internationale ontwikkelaars*

Used to obtain information about the capabilities of participants in the DSGO from the trust framework catalogue (provided by the trust framework authority). the `/capabilities` endpoint is used by all parties providing services within the context of the DSGO (data service providers, market facilities and the trust framework catalogue) to provide information about their service.

✔ Parties MUST provide information about their services via the `/capabilities` endpoint

Information about participants is provided in `capabilities_info` objects, as defined below.

## Capabilities_info object

**Note,** the DSGO follows the iSHARE /capabilities endpoint. We are in ongoing discussions to ensure the alignment of this endpoint with the requirements from the DSGO

| Parameters | | Type | Description |
|---|---|---|---|
| `party_id` | Required | String | Unique identifier of the party, MUST be an EORI number |
| `roles` | Required | Array of objects | Object containing an array of `role` objects hat provide the information about the roles of the party in the DSGO |
| `role` | Required | String in `roles` object | Role of the party. Available values are `DataServiceProvider`, `DataServiceConsumer`, `EntitledParty`, `AuthorisationRegistry`, `IdentityProvider`, `DataBroker` or `SchemeOwner` |
| `supported_versions` | | Array of objects | Contains information about supported version endpoints for each version. Contains `version` and `supported_features` |
| `version` | Required | String in `supported_versions` object | Version of the system which is under support |
| `supported_features` | Required | Array of objects in `supported_versions` object | Contains a list of supported features. Contains `public` and `restricted` objects. |
| `public` | Optional | Array of objects in `supported_features` object | Contains a list of public features (`id`, `feature`, `description`, `url` and `token_endpoint`) |
| `id` | Required | String in `public` object | Unique identifier of the feature. |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | `feature` | Required | String in `public` object | Friendly name of the feature. |
| | | | `description` | Required | String in `public` object | Short description about the feature. |
| | | | `url` | Required | String in `public` object | URL to the feature, according to RFC3986 |
| | | | `token_endpoint` | Optional | String in `public` object | URL where access token for the feature could be retrieved, according to RFC3986This is optional because if `feature` is `access token`, it is not needed to mention it twice. |
| | | `restricted` | | Optional | Array of objects in `supported_features` object | Contains supported restricted features. The structure and parameters are exactly the same as defined in `public` above (`id`, `feature`, `description`, `url` and `token_endpoint`). It should only be provided to the parties which provided a valid access token. If an access token was not provided or restricted endpoints does not exist, this value can be not returned and must be empty or null. |

Example capabilities_info object

```
"capabilities_info": {
    "party_id": "EU.EORI.NL000000003",
    "ishare_roles": [
      {
        "role": "Service Provider"
      }
    ],
    "supported_versions": [
      {
        "version": "1.7",
        "supported_features": [
          {
            "public": [
              {
                "id": "A51D413F-B3CC-477D-96C4-E37A9003BFE3",
                "feature": "capabilities",
                "description": "Retrieves iSHARE capabilities",
                "url": "https://w13.isharetest.net/capabilities",
                "token_endpoint": "https://w13.isharetest.net/connect/token"
              },
              {
                "id": "49F6E662-F055-4AAC-96B2-E833FA5F5414",
                "feature": "access token",
                "description": "Obtains access token",
                "url": "https://w13.isharetest.net/connect/token"
              },
              {
                "id": "05357B1C-A934-4BB2-A7CD-42948DA52379",
                "feature": "boom access",
                "description": "Request boom access based on user information",
                "url": "https://w13.isharetest.net/boom_access",
                "token_endpoint": "https://w13.isharetest.net/connect/token"
              },
```

```
            {
              "id": "105D19C7-02B1-481F-8B98-0C0F2F5EBB4B",
              "feature": "return client information",
              "description": "Displays identity of client to which access token was issued",
              "url": "https://w13.isharetest.net/me",
              "token_endpoint": "https://w13.isharetest.net/connect/token"
            }
          ]
        }
      ]
    }
  ]
}
```


## Endpoint

the `/parties` endpoint follows the generic technical requirements, as well as the requirements specified for specific methods. The figure below gives an overview of the HTTP methods that are supported by the `/parties` endpoint. These methods are further detailed and specified in the pages below:

- GET /capabilites

#### Visualize OpenAPI (Swagger) documentation app

Export to PDF of the OpenAPI specification is not supported. See interactive documentation online.

# GET /capabilites

Retrieves information about the features available to the requesting party

✔️ Parties MUST support a GET call to a `/capabilities` endpoint to retrieve a list of their features (in a `capabilities_info` object).

## Request

### Authorization

An access token may be used in GET calls to the `/capabilities` endpoint. For more information, see Access Token. The `/capabilities` endpoint should only return the public endpoints if no access token is provided. If an access token is provided, the `/capabilities` endpoint will also provide the restricted endpoints.

✔️ Parties MUST provide only `public` features to a successful GET request to the `/capabilities` endpoint, which does not include an access token

✔️ Parties MUST validate that a GET request to the `/capabilities` endpoint includes the `Authorization` headers and contains a valid access token, when returning `restricted` features

A party may also have private endpoints, which are endpoints for their own internal organization, also known as endpoints that are implemented, but not to share with the others. These endpoints are not within the scope of the DSGO and should not be returned to other parties.

### Parameters

For information about the parameters that are common to the trust framework's API's see Generic API Requirements.

Example request for a succesful GET /capabilities call

```
> Authorization: Bearer IIeDIrdnYo2ngwDQYJKoZIhvcNAQELBQAwSDEZMBcGA1UEAwwQaVNIQ

GET /capabilities
```

## Responses

### 200 OK

Successful, the response contains data providing the requested features of the party in a `capabilities_token`. The `capabilities_token` is a signed JWT, which contains the claims as defined in the Basic JWT, and additionally contains a `capabilities_info` object.

✔️ The trust framework catalogue MUST include a `capabilities_token` including a `capabilities_info` object in a response to a successful GET call to the `/capabilities` endpoint

Example of a response to a succesful GET /capabilities call

```
< Content-Type: application/json

{
  "capabilities_token": "eyJ4NWMiOlsiTUlJRWdUQ0NBbW1nQXdJQkFnSUlTOTBLKzFROUhPa3dEUVlKS29aSWh2Y05BUUVMQlFBd1NE
}
```

Decoded `capabilities_token` payload:


```
{
  "iss": "EU.EORI.NL000000003",
  "sub": "EU.EORI.NL000000003",
  "jti": "7071ecc5154441279903622af1bedbc0",
  "iat": 1591965277,
  "exp": 1591965307,
  "capabilities_info": {
    "party_id": "EU.EORI.NL000000003",
    "ishare_roles": [
      {
        "role": "Service Provider"
      }
    ],
    "supported_versions": [
      {
        "version": "1.7",
        "supported_features": [
          {
            "public": [
              {
                "id": "A51D413F-B3CC-477D-96C4-E37A9003BFE3",
                "feature": "capabilities",
                "description": "Retrieves iSHARE capabilities",
                "url": "https://w13.isharetest.net/capabilities",
                "token_endpoint": "https://w13.isharetest.net/connect/token"
              },
              {
                "id": "49F6E662-F055-4AAC-96B2-E833FA5F5414",
                "feature": "access token",
                "description": "Obtains access token",
                "url": "https://w13.isharetest.net/connect/token"
              },
              {
                "id": "05357B1C-A934-4BB2-A7CD-42948DA52379",
                "feature": "boom access",
                "description": "Request boom access based on user information",
                "url": "https://w13.isharetest.net/boom_access",
                "token_endpoint": "https://w13.isharetest.net/connect/token"
              },
              {
                "id": "105D19C7-02B1-481F-8B98-0C0F2F5EBB4B",
                "feature": "return client information",
                "description": "Displays identity of client to which access token was issued",
                "url": "https://w13.isharetest.net/me",
                "token_endpoint": "https://w13.isharetest.net/connect/token"
              }
            ]
          }
        ]
      }
```

```
    ]
  }
}
```

## 400 Bad Request

When `Authorization` header is provided, but the token format is invalid (for example, not `Bearer`).

## 401 Unauthorized

When `Authorization` header is either missing, invalid or the access token has already expired.

# Data service provider endpoints

*Deze pagina's zijn in het engels ten behoeve van mogelijk internationale ontwikkelaars*

The following endpoints and requirements are relevant for data service providers:

- API Service Content
- Example /resources
- /subscriptions

# API Service Content

*Deze pagina's zijn in het engels ten behoeve van mogelijk internationale ontwikkelaars*

Given the scope of the DSGO, the trust framework is data agnostic, and any type of content could be offered in data services. See Wat is een datadienst? for more information. It is the responsibility of the data service provider to determine the data resource offered in a data service in the data service definition. Although the data service provider is free to choose whatever data standard they see fit for their service, the DSGO presents the following agreement as a best practice.

✔ Data service providers SHOULD make use of relevant open standards in the definition of the service content of a data service

# Example /resources

*Deze pagina's zijn in het engels ten behoeve van mogelijk internationale ontwikkelaars*

A data service provider should define an endpoint for a resource in order to enable a specific data service in the DSGO. As the exact implementation of data service is highly dependent on the specific resource, the context, and the needs of the data service provider, no specific service is presented here. Only an example of a generic data service is presented for reference purposes. However, while implementing actual data services, all trust framework requirements apply:

✔ Data service providers MUST expose their resources in conformance with the trust framework API specifications

## Example /resources endpoint

This example is based on the requirements defined in the trust framework and allows various operations to be performed on a number of sample resources defined as a collection. The sample collection is defined as follows. It contains a list of different colours and their representative hex value, which can queried:

Note, this example includes a small amount of JSON formatted data. As the trust framework is data standard agnostic, this could be any format, including XML or Base64 encoded data.

```
[{
  "id": "001",
  "data": {
    "colour": "red",
    "value": "#f00",
    "description": "Hex value of the colour red"
  }
}, {
  "id": "002",
  "data": {
    "colour": "green",
    "value": "#0f0",
    "description": "Hex value of the colour green"
  }
}, {
  ...
}]
```

#### Visualize OpenAPI (Swagger) documentation app

Export to PDF of the OpenAPI specification is not supported. See interactive documentation online.

# /subscriptions

*Deze pagina's zijn in het engels ten behoeve van mogelijk internationale ontwikkelaars*

Subscriptions allow data service consumers to get notifications for specific events as defined by a data service provider. Within the trust framework, subscriptions are managed in phases, find more information in the lifecycle of subscriptions. The subscription resource has been defined to structure all relevant parameters of these elements and available actions throughout the lifecycle of a subscription. If data service providers decide a subscription is applicable to their situation, this must be implemented in accordance to the resources as defined here.

✔️ Data service providers MUST define subscriptions for events in accordance to the `subscription` resource, when implementing a subscription

✔️ Data service providers MUST define events for their subscriptions in accordance to the `events` resource, when implementing a subscription

## Subscription resource

| Parameters | | Description |
|---|---|---|
| `id` | Required | Unique identifier of the subscription |
| `resource_type` | Required | String representing the resource type, equal to `subscription` |
| `href` | Required | URL of the subscription, according to RFC3986 |
| `created_date` | Required | Date time when the subscription was initially created, according to ISO 8601 |
| `start_date` | Required | Contains the date time when the subscription becomes/became valid, according to ISO 8601 |
| `end_date` | Optional | If the subscription has an end date, or has ended, contains the end date and time, according to ISO 8601 |
| `consumer_id` | Required | If the subscription is assigned a data service consumer contains a unique identifier of the data service consumer as an EORI number |
| `provider_id` | Required | Unique identifier of the data service provider as an EORI number |
| `description` | Optional | Description of the subscription |
| `event_type` | Required | List with subset of event types that is subscribed to, selected from the list defined by the data service provider |
| `status` | Required | Status of the subscription. Possible values are: `active`, `inactive`. See the lifecycle of a subscription for more information |

| | | |
|---|---|---|
| `webhook_url` | Required | URL of the data service consumer that notifications shall be sent to, according to RFC3986 |

Example of an subscription object

```
{
  "id": "sub_123",
  "resource_type": "subscription",
  "href": "/subscriptions/sub_123",
  "created_date": "2022-09-21T10:23:37Z",
  "start_date": "2022-09-21T23:59:59Z",
  "end_date": "2023-09-21T23:59:59Z",
  "consumer_id": "EU.EORI.NL000123456",
  "provider_id": "EU.EORI.NL000345678",
  "description": "detailed description of the subscription",
  "event_type": ["Modified,","Deleted"],
  "status": "active",
  "webhook_url": "https://example.com/notifications"
}
```

## Endpoint

The `/subscriptions` endpoint allows data service consumers to perform a number of different functions on the subscriptions defined by a data service provider. All subscriptions APIs should follow the generic technical requirements, as well as the requirements specified for specific methods. Further, data service providers are responsible for determining a suitable authorisation policy for their subscriptions. See Autorisatie for more information.

✔️ Data service providers MUST expose their subscriptions in conformance with the DSGO `/subscriptions` endpoint specifications

✔️ Data service providers MUST determine suitable authorisation policy for their `/subscriptions` endpoint

The figure below gives an overview of the HTTP methods that are supported by the `/subscriptions` endpoint. These methods are further detailed and specified in the pages below:

- Lifecycle of a Subscription
- GET /subscriptions
- POST /subscriptions
- GET /subscriptions/{id}
- DELETE /subscriptions/{id}
- POST /subscriptions/{id}/test

**Visualize OpenAPI (Swagger) documentation app**

Export to PDF of the OpenAPI specification is not supported. See interactive documentation online.

# Lifecycle of a Subscription

Within the DSGO, subscriptions are managed in simple phases. In the figure below, the different phases in the lifecycle of a subscription are presented. The phase that a subscription is in is indicated in the `status` field of a subscription resource. The table below gives a description of each phase, and describes the behaviour of a subscription in the phase.

Note that in the future, in the further development of the trust framework it is deemed necessary to increase the functionality of subscriptions, the lifecycle may be further expanded with additional phases.


Overview of the lifecycle of subscriptions within the trust framework

| Status | Description |
| --- | --- |
| `active` | The data service consumer has subscribed to the defined events and will receive notifications from the data service provider in accordance with the subscription as defined by the data service provider. |
| `inactive` | Due to a wide range of possible actions by either the data service consumer or data service provider, the subscription has been deactivated. This can occur for example if the subscription has expired or been cancelled by the data service consumer. |

# GET /subscriptions

Retrieves a list of all subscriptions have been made accessible to a data service consumer by a data service provider. This may include subscriptions at any phase in their lifecycle.

✔️ Data service providers MUST support a GET call to a `/subscriptions` endpoint to retrieve a list of available subscriptions

## Request

### Authorisation

The data service provider is responsible for determining a suitable authorisation policy for their subscriptions resources. See Autorisatie for more information.

### Parameters

For information about the parameters that are common to the trust framework's API's see Generic API Requirements, and for parameters common to all subscriptions methods, see /subscriptions.

## Responses

### 200 OK

Successful, the response body contains data providing a list of subscriptions available to the data service consumer. The data is structured as an array of subscription resources as indicated in the example below:

✔️ Data service providers MUST include a list of subscription resources available for the data service consumer in a response to a successful GET calls to the `/subscriptions` endpoint

✔️ Data service providers MUST provide a count of the number of subscriptions included, in the `count` parameter, in the response to a successful GET calls to the `/subscriptions` endpoint

Example response body for a succesful GET /subscriptions call


```
{
  "count": 4,
  "subscriptions": [
    {
      "id": "sub_123",
      "class": "subscription",
      "href": "/subscriptions/sub_123",
      "created_date": "2022-09-21T10:23:37Z",
      "start_date": "2022-09-21T23:59:59Z",
      "end_date": "2023-09-21T23:59:59Z",
      "consumer_id": "EU.EORI.NL000123456",
      "provider_id": "EU.EORI.NL000345678",
      "description": "detailed description of the subscription",
      "event_type": ["Modified"],
```

```
      "status": "active",
      "webhook_url": "https://example.com/notifications"
    },
    {
      "id": "sub_345",
      "class": "subscription",
      "href": "/subscriptions/sub_345",
      "created_date": null,
      "start_date": null,
      "end_date": null,
      "consumer_id": null,
      "provider_id": "EU.EORI.NL000345678",
      "description": "detailed description of the subscription",
      "event_type": ["Modified","Deleted"]
      "status": "inactive",
      "webhook_url": null
    },
    {...},
    {...},
  ]
}
```

# POST /subscriptions

Creates a new subscription for a data service consumer at a data service provider. This method results in a subscription with `status` set to `active`. (see Lifecycle of a Subscription for more information)

✔️ Data service providers MUST support a POST call to a `/subscriptions` endpoint to create a new subscription

## Request

### Authorisation

The data service provider is responsible for determining a suitable authorisation policy for their subscriptions resources. See Autorisatie for more information.

### Parameters

For information about the parameters that are common to the trust framework's API's see Generic API Requirements, and for parameters common to all subscriptions methods, see /subscriptions. The HTTP body must contain a subscription resource, in accordance to the subscription as defined by the data service provider.

✔️ Data service providers MUST validate that the HTTP body of a POST request to a `/subscriptions` endpoint contains the following parameters, with content as defined in the `subscription` resource:

- `class`
- `start_date` (optional)
- `end_date` (optional)
- `event_type`
- `webhook_url`

✔️ Data service providers MUST validate that a POST request to `/subscriptions` endpoint complies with their data service specific subscription requirements

Example request body for a POST /subscriptions call

```
{
  "class": "subscription",
  "created_date": "2022-09-21T10:23:37Z",
  "start_date": "2022-09-21T23:59:59Z",
  "end_date": null,
  "event_type": ["Modified"],
  "webhook_url": "https://example.com/notifications"
}
```

# Responses

## 201 Created

Successful, the new subscription is created. The response body contains the data of the created subscription as a `subscription` resource, as indicated in the example below:

✔️ Data service providers MUST respond with a `201 Created` to a successful POST call to a `/subscriptions` endpoint

✔️ Data service providers MUST include the created `subscription` resource in the HTTP body of the response to a successful POST call to the `/subscriptions` endpoint

Example response body for a succesful POST /subscriptions call

```
{
  "id": "sub_123",
  "class": "subscription",
  "href": "/subscriptions/sub_123",
  "created_date": "2022-09-21T10:23:37Z",
  "start_date": "2022-09-21T23:59:59Z",
  "end_date": "2023-09-21T23:59:59Z",
  "consumer_id": "EU.EORI.NL000123456",
  "provider_id": "EU.EORI.NL000345678",
  "description": "detailed description of the subscription",
  "event_type": ["Modified"],
  "status": "active",
  "webhook_url": "https://example.com/notifications"
}
```

# GET /subscriptions/{id}

Retrieves the information of a specific subscription with the given ID at a data service provider.

✔️ Data service providers MUST support a GET call to a `/subscriptions/{id}` endpoint to get information about a specific subscription

## Request

### Authorisation

The data service provider is responsible for determining a suitable authorisation policy for their subscriptions resources. See Autorisatie for more information.

### Parameters

For information about the parameters that are common to trust framework's API's see Generic API Requirements, and for parameters common to all subscriptions methods, see /subscriptions.

✔️ Data service providers MUST validate that the `{id}` of a GET request to a `/subscriptions/{id}` is valid, exists and is available to the data service consumer

## Responses

### 200 OK

Successful, the response body contains data of the specific subscription requested. The data has to be structured as a `subscription` resource, as indicated in the example below.

✔️ Data service providers MUST respond with a 200 OK to a successful GET call to a `/subscriptions/{id}` endpoint

✔️ Data service providers MUST include the requested `subscription` resource in the HTTP body of the response to a successful GET call to the `/subscriptions/{id}` endpoint

Example response body for a succesful GET /subscriptions/sub_123 call

```
{
  "id": "sub_123",
  "class": "subscription",
  "href": "/subscriptions/sub_123",
  "created_date": "2022-09-21T10:23:37Z",
  "start_date": "2022-09-21T23:59:59Z",
  "end_date": "2023-09-21T23:59:59Z",
  "consumer_id": "EU.EORI.NL000123456",
  "provider_id": "EU.EORI.NL000345678",
  "description": "detailed description of the subscription",
  "event_type": ["Modified"],
```

```
  "status": "active",
  "webhook_url": "https://example.com/notifications"
}
```

## 404 Not found

✔️ Data service providers MUST respond with a 404 Not found to a GET call to a `/subscriptions/{id}` endpoint when the `{id}` is not valid or available to a data service consumer

# DELETE /subscriptions/{id}

Removes a specific subscription with the given ID at a data service provider. This method is possible on all subscriptions with `status` equal to `active` and results in their `status` being set to `inactive` such that they cannot be used. (see Lifecycle of a Subscription for more information)

✔️ Data service providers MUST support a DELETE call to a `/subscriptions/{id}` endpoint to remove a specific subscription

## Request

### Authorisation

The data service provider is responsible for determining a suitable authorisation policy for their subscriptions resources. See Autorisatie for more information.

### Parameters

For information about the parameters that are common to the trust framework's API's see Generic API Requirements, and for parameters common to all subscriptions methods, see /subscriptions.

✔️ Data service providers MUST validate that the `{id}` of a DELETE request to a `/subscriptions/{id}` is valid, exists and is available to the data service consumer

✔️ Data service providers MUST validate that the `subscription` resource being deleted complies with their data service specific subscription requirements

## Responses

### 200 OK

Successful, the subscription is deleted.

✔️ Data service providers MUST respond with a 200 OK to a successful DELETE call to a `/subscriptions/{id}` endpoint

✔️ Data service providers MUST NOT include an HTTP body in the response to a successful DELETE call to the `/subscriptions/{id}` endpoint

✔️ Data service providers MUST set the `“status"` of `subscription/{id}` to `"inactive"` in response to a successful DELETE call to the `/subscriptions/{id}` endpoint

### 404 Not found

✔️

Data service providers MUST respond with a 404 Not found to a DELETE call to a `/subscriptions/{id}` endpoint when the `{id}` is not a valid or available to the data service consumer

# POST /subscriptions/{id}/test

Triggers the sending of a test notification by a data service provider to a data service consumer for an existing subscription with the given ID. This method is only possible on subscriptions with `status` equal to `active` (see Lifecycle of a Subscription for more information)

✔️ Data service providers MUST support a POST call to a `/subscriptions/{id}/test` endpoint to send a test notification to the data service consumers supplied /notifications endpoint

## Request

### Authorisation

The data service provider is responsible for determining a suitable authorisation policy for their subscriptions resources. See Autorisatie for more information.

## Parameters

For information about the parameters that are common to the trust framework's API's see Generic API Requirements, and for parameters common to all subscriptions methods, see /subscriptions.

✔️ Data service providers MUST validate that the HTTP body of a POST request to a `/subscriptions/{id}/test` endpoint is empty

✔️ Data service providers MUST validate that the `{id}` of a POST request to a `/subscriptions/{id}/test` is valid, exists and is available to the data service consumer

## Responses

### 202 Accepted

Successful, triggers the sending of a test notification to the data service consumer

✔️ Data service providers MUST respond with a 202 Accepted to a successful POST call to a `/subscriptions/{id}/test` endpoint

✔️ Data service providers MUST NOT include an HTTP body in the response to a successful POST call to the `/subscriptions/{id}/test` endpoint

✔️ Data service providers MUST trigger the sending of a `notification` with `“eventType":“Test"` to the subscription's webhook `url` in response to a successful POST call to the `/subscriptions/{id}/test` endpoint

### 404 Not found

✔️ Data service providers MUST respond with a 404 Not found to a POST call to a `/subscriptions/{id}/test` endpoint when the `{id}` is not a valid or available to the data service consumer

# Data service consumer endpoints

*Deze pagina's zijn in het engels ten behoeve van mogelijk internationale ontwikkelaars*

The following endpoints are relevant for data service consumers.

- /notifications

# /notifications

*Deze pagina's zijn in het engels ten behoeve van mogelijk internationale ontwikkelaars*

In order for a data service consumer to subscribe to an event as defined by a data service provider, they must be able to receive notifications containing events via a `/notifications` endpoint. Notifications are only sent for subscriptions with `status` equal to `active` (see Lifecycle of a Subscription for more information). Notifications and events are always structured according to the `notification`, and `event` objects.

✔ Data service consumers MUST have an `/notifications` endpoint implemented before obtaining a subscription

✔ Data service consumers MUST support a `notification` object

## Notification object

| Parameters | | Description |
|---|---|---|
| `id` | Required | Unique identifier of the notification |
| `resource_type` | Required | String representing the object type, equal to `notification` |
| `date` | Required | Date and time that the notification was sent, according to ISO 8601 |
| `consumer_id` | Required | Unique identifier of the data service consumer as an EORI number |
| `provider_id` | Required | Unique identifier of the data service provider as an EORI number |
| `subscription_id` | Required | Unique identifier of the subscription under which the event is monitored |
| `description` | Optional | Description of the notification |
| `event` | Required | event object, as defined here, containing data regarding the event which triggered the notification |

Example notification object

```
{
  "id" : "not_123",
  "resource_type" : "notification",
  "date" : "2022-09-21T10:23:48Z",
  "consumer_id" : "EU.EORI.NL000123456",
  "provider_id" : "EU.EORI.NL000345678",
  "subscription_id" : "sub_123",
  "description" : "Detailed description of the notification",
  "event" : [
    {
      "id" : "eve_123",
      "object_type" : "event",
```

```
      "event_type" : "Modified",
      "date" : "2022-09-21T10:23:37Z",
      "description" : "Detailed description of the event",
      "event_data" : "Data record xyz has been modified by zyx"
    }
  ]
}
```

## Event object

| Parameters | | Description |
|---|---|---|
| `id` | Required | Unique identifier of the event |
| `resource_type` | Required | String representing the object type, equal to `event` |
| `event_type` | Required | Label of the type of event that has taken place. Exact values to be defined by a specific data service. For example: `Modified`, `Deleted`, `Moved`, `Created` |
| `date` | Required | Date and time that the event took place, according to ISO 8601 |
| `description` | Optional | Detailed description of the event |
| `event_data` | Optional | Optional data related to the event |

Example of an event object

```
{
  "id" : "eve_123",
  "resource_type" : "event",
  "event_type" : "Modified",
  "date" : "2022-09-21T10:23:37Z",
  "description" : "Detailed description of the event",
  "event_data" : "Data record xyz has been modified by zyx"
}
```

## Endpoint

The `/notifications` endpoint allows data service consumers to receive and act upon notifications from a data service provider. The notifications APIs should follow the generic technical requirements, as well as the requirements specified for specific methods. Further, data service consumers are responsible for determining a suitable authorisation policy for their notifications. See Autorisatie for more information.

✔️ Data service consumers MUST expose their subscriptions in conformance with the DSGO `/notifications` endpoint specifications

✔️ Data service consumers MUST determine suitable authorisation policy for their `/notifications` endpoint

The figure below gives an overview of the HTTP methods that are supported by the `/notifications` endpoint. These methods are further detailed and specified in the pages below:

- POST /notifications

**Visualize OpenAPI (Swagger) documentation app**

Export to PDF of the OpenAPI specification is not supported. See interactive documentation online.

# POST /notifications

A notification sent by a data service provider to a data service consumer in accordance to an existing subscription.

✔️ Data service consumers MUST support a POST call to a `/notifications` endpoint to be able to receive notifications from data service providers

## Request

### Authorisation

The data service consumer is responsible for determining a suitable authorisation policy for their notifications resources. See Autorisatie for more information.

### Parameters

For information about the parameters that are common to the trust framework's API's see Generic API Requirements, and for parameters common to all notification methods, see /notifications.

✔️ Data service consumers MUST validate that the HTTP body of a POST request to a `/notifications` endpoint contains a valid `notification` object

Example request body for a POST /notifications call

```
{
  "id" : "not_123",
  "resource_type" : "notification",
  "date" : "2022-09-21T10:23:48Z",
  "consumer_id" : "EU.EORI.NL000123456",
  "provider_id" : "EU.EORI.NL000345678",
  "subscription_id" : "sub_123",
  "description" : "Detailed description of the notification",
  "event" : [
    {
      "id" : "eve_123",
      "resource_type" : "event",
      "event_type" : "Modified",
      "date" : "2022-09-21T10:23:37Z",
      "description" : "Detailed description of the event",
      "event_data" : "Data record xyz has been modified by zyx
    }
  ]
}
```

# Responses

## Authorisation

The data service provider is responsible for determining a suitable authorisation policy for the response to a sent notification. See Autorisatie for more information. Due to possible non-repudiation requirements for notifications, responses to notifications may require authentication and authorisation

## 200 OK

Successful, confirmation that the notification has been received

✔️ Data service consumer MUST respond with a 200 OK to a successful POST call to a `/notification` endpoint

# Trust framework catalogue endpoints

*Deze pagina's zijn in het engels ten behoeve van mogelijk internationale ontwikkelaars*

The following endpoints and requirements are relevant for the Trust Framework Catalog:

- /parties
- /trusted_list

# /parties

*Deze pagina's zijn in het engels ten behoeve van mogelijk internationale ontwikkelaars*

Used to obtain information about participants in the DSGO from the trust framework catalogue (provided by the trust framework authority). The `/parties` endpoint is available to verify the status of participants.

The trust framework catalogue MUST provide information about participants via the `/parties` endpoint

Information about participants is provided in `party_info` objects, as defined below.

## Parties_info object

| Parameters | | | Type | Description |
|---|---|---|---|---|
| `party_id` | | Required | String | Unique identifier of the party, MUST be an EORI number |
| `party_name` | | Required | String | String representing the object type, equal to `notification` |
| `adherance` | | Required | Object | Object containing the `status`, and validity timestamps (`start_date` and `end_date`) |
| | `status` | Required | String in `adherance` object | Unique identifier of the data service consumer as an EORI number |
| | `start_date` | Required | String in `adherance` object | Date and time which states since when the adherence status has established, according to ISO 8601 |
| | `end_date` | Required | String in `adherance` object | Date and time which states till when the adherence status is established, according to ISO 8601 |
| `certifications` | | Required | Object | Object containing a collection of the certifications of the party indicating what market facility role(s) the party fulfils (the `role`, `start_date`, `end_date` and `loa`) |
| | `role` | Required | String in `certifications` object | Role of acquired certification. Available values are `AuthorisationRegistry`, `IdentityProvider`, `dataBroker` or `SchemeOwner`. |
| | `start_date` | Required | String in `certifications` object | Date and time which states since when the certification has been established, according to ISO 8601 |
| | `end_date` | Required | String in `certifications` object | Date and time which states till when the certification is established, according to ISO 8601 |

| | | | | |
|---|---|---|---|---|
| | `loa` | Required | Integer in `certifications` object | Certificate's level of assurance. Available values are `1` (low), `2` (substantial) and `3` (high) |
| `capability_url` | | Required | String | `/capabilities` endpoint of the party, according to RFC3986. See /capabilities for more information |

Example parties_into object

```
"party_info": {
  "party_id": "EU.EORI.NL000000004",
  "party_name": "AskMeAnything Authorization Registry",
  "adherence": {
    "status": "Active",
    "start_date": "2018-04-26T00:00:00",
    "end_date": "2020-07-25T00:00:00"
  },
  "certifications": [
    {
      "role": "AuthorisationRegistry",
      "start_date": "2018-01-04T00:00:00",
      "end_date": "2020-02-02T00:00:00",
      "loa": 3
    }
  ],
  "capability_url": "https://ar.isharetest.net/capabilities"
}
```

## Endpoint

the `/parties` endpoint follows the generic technical requirements, as well as the requirements specified for specific methods. The figure below gives an overview of the HTTP methods that are supported by the `/parties` endpoint. These methods are further detailed and specified in the pages below:

- GET /parties

#### Visualize OpenAPI (Swagger) documentation app

Export to PDF of the OpenAPI specification is not supported. See interactive documentation online.

# GET /parties

Retrieves a list of all participants to the requesting party from the trust framework catalogue.

✔️ The trust framework catalogue MUST support a GET call to a `/parties` endpoint to retrieve a list of DSGO participants (in an array of `parties_info` objects).

## Request

### Authorization

the `/parties` endpoint is publicly available to all parties

### Parameters

For information about the parameters that are common to the trust framework's API's see Generic API Requirements.

✔️ The trust framework catalogue MUST validate that the HTTP body of a GET request to the `/parties` endpoint contains the parameters as defined in the table below

✔️ The trust framework catalogue MUST validate that the HTTP body of a GET request to the `/parties` endpoint contains at least a single parameter.

| Parameter | | Type | Description |
|---|---|---|---|
| `name` | Optional | String | Used to search by a party's name. Can contain a single `*` as wildcard |
| `eori` | Optional | String | Used to search by a party's EORI. Can contain a single `*` as wildcard |
| `certified_only` | Optional | Boolean | Used to search all certified parties. If null is provided, then it will not affect the query and will return both certified and non-certified parties. If false is provided, then the query will return non-certified parties. If true is provided, the query will return certified parties. |
| `active_only` | Optional | Boolean | Used to search all active parties. If null is provided, then it will not affect the query and will return both active and inactive parties. If false is provided, then the query will return inactive parties. If true is provided, then the query will return active parties. |
| `certificate_subject_name` | Optional | Boolean | `subjectName` as encoded in the X.509 certificate, which corresponds with the party that is being requested from the trust framework catalogue. Used by the catalogue to match the certificate identifier. Subject name attributes may be in any order, but all of them must be included and separated by |

| | | | |
|---|---|---|---|
| | | | comma, if at least one subject attribute is missing - information won't be returned. Only returns info if combined with the valid `eori` associated to it. |
| `page` | Optional | Integer | Used for navigation in case the result contains more than 10 parties. |
| `date_time` | Optional | String | Date and time for which the information is requested. MUST contain a timestamp, formatted according to UTC. If provided, the result becomes final and therefore MUST be cacheable. |

Example request body for a succesful GET /parties call

```
> Authorization: Bearer IIeDIrdnYo2ngwDQYJKoZIhvcNAQELBQAwSDEZMBcGA1UEAwwQaVNIQ

GET /parties?
    eori=EU.EORI.NL000000004&
    certificate_subject_name=C=NL, SERIALNUMBER=EU.EORI.NL000000004, CN=iSHARE Test Authorization Registry&
    active_only=true
```

# Responses

## 200 OK

Successful, the response contains data providing the requested parties information in a `party_token`. The `party_token` is a signed JWT, which contains the claims as defined in the Basic JWT, and additionally contains a `parties_info` object.

✔ The trust framework catalogue MUST include a `party_token` including of an (array of) `parties_info` objects in a response to a successful GET calls to the `/parties` endpoint

Example of a response to a succesful GET /parties call

```
< Content-Type: application/json

{
  "party_token": "eyJ4NWMiOlsiTUlJRWlEQ0NBbkNnQXdJQkFnSUllRElyZG5ZbzJuZ3dEUVlKS29aSWh2Y05BUUVMQlFBd1NERVpNQmN
}
```

Decoded `party_token` payload:

```
{
  "iss": "EU.EORI.NL000000000",
  "sub": "EU.EORI.NL000000000",
  "jti": "77e8179fbfe6469eb64c054da26a77c3",
  "iat": 1589282112,
  "exp": 1589282142,
  "aud": "EU.EORI.NL000000001",
  "party_info": {
    "party_id": "EU.EORI.NL000000004",
    "party_name": "AskMeAnything Authorization Registry",
    "adherence": {
      "status": "Active",
      "start_date": "2018-04-26T00:00:00",
      "end_date": "2020-07-25T00:00:00"
    },
```

```
    "certifications": [
      {
        "role": "AuthorisationRegistry",
        "start_date": "2018-01-04T00:00:00",
        "end_date": "2020-02-02T00:00:00",
        "loa": 3
      }
    ],
    "capability_url": "https://ar.isharetest.net/capabilities"
  }
}
```


## 400 Bad Request

When `Authorization` header is provided, but the token format is invalid (for example, not `Bearer`). Additionally, a `400` should be returned when the provided access token  is valid, but query parameters are either invalid or none of them were provided.

## 401 Unauthorized

When `Authorization` header is either missing, invalid or the access token has already expired.

# /trusted_list

*Deze pagina's zijn in het engels ten behoeve van mogelijk internationale ontwikkelaars*

Used to obtain a list of trusted certificate authorities which are trusted within the DSGO from the trust framework catalogue (provided by the trust framework authority). The `/trusted_list` endpoint returns all eIDAS-qualified certificate authorities which are valid under DSGO.

✔ The trust framework catalogue MUST provide information about trusted certificate authorities via the `/trusted_list` endpoint

Information about participants is provided in `trusted_list` objects, as defined below.

## Trusted_list object

| Parameters | | Type | Description |
|---|---|---|---|
| `subject` | Required | String | Certificate authority subject name |
| `certificate_fingerprint` | Required | String | SHA256 fingerprint of the certificate |
| `validity` | Required | Object | Validity of the certificate. MUST contain the value `valid` or `invalid` |
| `status` | Required | Object | Status of the certificate. MUST contain the value `granted`, `withdrawn`, `supervisionceased` or `undersupervision` |

Example trusted_list object

```
{
  "subject": "C=NL, O=Staat der Nederlanden, CN=TEST Staat der Nederlanden Organisatie Services CA - G3",
  "certificate_fingerprint": "DC13FC94FF0149DE1B07F7965F655AED54C6A6BDA7ADF71A732FFCFABC454C7A",
  "validity": "valid",
  "status": "granted"
},
```

## Endpoint

the `/trusted_list` endpoint follows the generic technical requirements, as well as the requirements specified for specific methods. The figure below gives an overview of the HTTP methods that are supported by the `/trusted_list` endpoint. These methods are further detailed and specified in the pages below:

- GET /trusted_list

**Visualize OpenAPI (Swagger) documentation app**

Export to PDF of the OpenAPI specification is not supported. See interactive documentation online.

# GET /trusted_list

Retrieves a list of all certificate authorities which are trusted within the DSGO to the requesting party from the trust framework catalogue.

✔️ The trust framework catalogue MUST support a GET call to a `/trusted_list` endpoint to retrieve a list of DSGO participants (in an array of `trusted_list` objects).

## Request

### Authorization

the `/parties` endpoint is publicly available to all parties.

### Parameters

For information about the parameters that are common to the trust framework's API's see Generic API Requirements.

Example request for a succesful GET /trusted_list call

```
> Authorization: Bearer IIeDIrdnYo2ngwDQYJKoZIhvcNAQELBQAwSDEZMBcGA1UEAwwQaVNIQ

GET /trusted_list
```

## Responses

### 200 OK

Successful, the response contains data providing the requested list of trusted certificate authorities requested parties information in a `trusted_list_token`. The `trusted_list_token` is a signed JWT, which contains the claims as defined in the Basic JWT, and additionally contains an array of `trusted_list` objects.

✔️ The trust framework catalogue MUST include a `trusted_list_token` including of an (array of) `trusted_list` objects in a response to a successful GET calls to the `/trusted_list` endpoint

Example of a response to a succesful GET /trusted_list call

```
< Content-Type: application/json

{
  "trusted_list_token": "eyJ4NWMiOlsiTUlJRWlEQ0NBbkNnQXdJQkFnSUllRElyZG5ZbzJuZ3dEUVlKS29aSWh2Y05BUUVMQlFBd1NE
}
```

Decoded `trusted_list_token` payload:

```
{
  "iss": "EU.EORI.NL000000000",
  "sub": "EU.EORI.NL000000000",
```

```
  "jti": "9774d924b8c04b97bd3f0807deb154b6",
  "iat": 1591966010,
  "exp": 1591966040,
  "aud": "EU.EORI.NL000000001",
  "trusted_list": [
    {
      "subject": "C=NL, O=Staat der Nederlanden, CN=TEST Staat der Nederlanden Organisatie Services CA - G3"
      "certificate_fingerprint": "DC13FC94FF0149DE1B07F7965F655AED54C6A6BDA7ADF71A732FFCFABC454C7A",
      "validity": "valid",
      "status": "granted"
    },
    {
      "subject": "C=NL, O=iSHARE Foundation, CN=TEST iSHARE Foundation PKIoverheid Organisatie Server CA - G
      "certificate_fingerprint": "F218133CD3AC2D970D10CA46BB03F832453324B0F4AF5C3F61BAD6FDEEC5EB83",
      "validity": "valid",
      "status": "granted"
    },
    {
      "subject": "C=NL, O=TEST Staat der Nederlanden, CN=TEST Staat der Nederlanden Root CA - G3",
      "certificate_fingerprint": "98C9C14F7F1F9A83A744E0ACBA9DA6A47EE96E053D72795457A5BC0207229D43",
      "validity": "valid",
      "status": "granted"
    },
    {
      "subject": "CN=TEST iSHARE Foundation eIDAS",
      "certificate_fingerprint": "8C39DD06E35DE8467004A542D0CA4B8FDC7D6F8F713F40A35BD9E65938A191CF",
      "validity": "valid",
      "status": "granted"
    },
    {
      "subject": "C=NL, O=iSHARE, OU=Test, CN=iSHARETestCA",
      "certificate_fingerprint": "A78FDF7BA13BBD95C6236972DD003FAE07F4E447B791B6EF6737AD22F0B61862",
      "validity": "valid",
      "status": "granted"
    },
    {
      "subject": "CN=TEST iSHARE EU Issuing Certification Authority G5",
      "certificate_fingerprint": "FD5593DC874ECC1133C21A77259C3592552EC0C89DFCD7AB3C0BDCFD73F0F5CC",
      "validity": "valid",
      "status": "granted"
    },
    {
      "subject": "C=NL, O=iSHARE, OU=Test, CN=iSHARETestCA_TLS",
      "certificate_fingerprint": "DF2FF51D1B2559D686723C97037DC9D5C589406CAC4F84C29AB3D43E0126251D",
      "validity": "valid",
      "status": "granted"
    }
  ]
}
```


## 401 Unauthorized

When `Authorization` header is either missing, invalid or the access token has already expired.

# Identificatie

Identificatie is in het kader van DSGO het proces waarbij een identiteit wordt toegekend aan of wordt geclaimd door een partij die een rol vervult in het afsprakenstelsel. Bij het uitvoeren van een datadienst tussen een datadienstaanbieder en datadienstgebruiker met toestemming van de rechthebbende is het van belang dat de identiteit van alle betrokken partijen waarmee geïnteracteerd wordt vastgelegd.

⭐ **Voorbeeld**: In een setting waar sensor data van een brug wordt gedeeld met onderhoudspartijen t.b.v. preventief onderhoud, moeten de volgende partijen worden geïdentificeerd binnen de context van een datadienst:

- De onderhoudspartijen als datadienstgebruikers
  - Werknemer van de onderhoudspartij die namens zijn werkgever toegang heeft tot de software die gebruik maakt van de datadienst
- De sensor leveranciers als datadienstaanbieders

Binnen de context van een datadienst zijn er twee verschillende soorten partijen betrokken die rollen kunnen innemen:

| Term | Omschrijving |
|---|---|
| Organisatie | een bedrijf, (overheids-)instelling of vereniging |
| Persoon | een natuurlijk persoon, een mens |

Voor beide type partijen (organisaties en personen) zijn afspraken gemaakt.

- Identificatie van Organisaties
- Identificatie van Personen

## Identificerend kenmerk

Een identiteit wordt zoveel mogelijk uitgedrukt met een identificerend kenmerk.

ℹ️ Voor het identificeren van mensen in de context van de gebouwde omgeving zal in de meeste gevallen geen BSN of ander uniek identificerend kenmerk mogen worden gebruikt. Als alternatief kunnen hier use case specifieke pseudoniemen of uniek identificerende attribuutsets worden gebruikt. Dit moet nader worden onderzocht.

⭐ **Voorbeeld**: Het Rechtspersonen en Samenwerkingsverbanden Informatienummer (RSIN) is een identificerend kenmerk voor alle rechtspersonen en samenwerkingsverbanden, zoals bv's, verenigingen, stichtingen, vof's en maatschappen die bij de KVK zijn ingeschreven. Dit nummer wordt gebruikt bij het uit wisselen van gegevens met andere (overheids)organisaties, zoals de Belastingdienst. Omdat het RSIN nummer uniek is, kan een rechtspersoon deze gebruiken om haar identiteit te claimen en kan de ontvanger bepalen welke persoon het is.

✔️ Partijen MOETEN zich uniek identificeren wanneer ze betrokken zijn bij een datadienst

✔️ Partijen MOETEN andere partijen die betrokken zijn bij een datadienst uniek identificeren

## Scope identificatie

Binnen de context van een datadienst zijn veel elementen betrokken die op dat moment niet zelfstandig handelen en dus geen rol binnen het DSGO spelen. Bijvoorbeeld ramen, balken, IoT sensoren, prefab muren en slimme meters.

Binnen datasets kan het zijn dat een object uniek identificeerbaar moeten zijn in de context van de datadienst o.b.v. één identificeerbaar kenmerk. Omdat dit een onderdeel is van de datadienstdefinitie is dit de verantwoordelijkheid van de datadienstaanbieder, en niet in scope van het afsprakenstelsel.

⭐ **Voorbeeld**: In dezelfde setting waar sensor data van een brug wordt gedeeld met onderhoudspartijen t.b.v. preventief onderhoud, moeten de volgende objecten waarschijnlijk identificeerbaar zijn, maar dat is, tenzij daar aanvullende afspraken over zijn gemaakt, buiten scope van DSGO en dus volledig aan de datadienstaanbieder:

- Individuele sensoren die data genereren
- De brug of onderdelen van de brug die onderhouden moeten worden

### IoT objecten

Het ‘internet of things’ (IoT) is een netwerk van fysieke objecten met sensoren, verwerkingscapaciteit, software of andere technologieën die verbonden zijn met het internet om data uit te wisselen. IoT objecten kunnen bijvoorbeeld een dataset genereren die een datadienstaanbieder beschikbaar stelt aan een datadienstgebruiker middels een datadienst. Het is van belang dat een datadienstaanbieder de IoT objecten kan identificeren en, indien nodig, communiceren met de datadienstgebruiker. Maar, omdat het IoT object niet direct betrokken is bij de datadienst (de datadienstgebruiker ‘praat’ niet direct met het object), is het niet van belang dat het IoT object wordt geïdentificeerd in de datadienst. Daarom worden geen additionele afspraken voorzien betreffende de identificatie van IoT objecten.

# Identificatie van Organisaties

Voor een gestandaardiseerde identificatie van organisaties gebruikt het afsprakenstelsel een EORI-nummer ("Economic Operators Registration and Identification number"). Dit is een binnen de gehele EU veelgebruikte identificerend kenmerk voor organisaties en het is ook te verkrijgen door organisaties van buiten de EU.

✔️ Partijen MOETEN het EORI-nummer gebruiken als uniek identificerend kenmerk voor organisaties

**Toelichting keuze EORI-nummer**

De Europese wetgever heeft het identificerend kenmerk voor juridische entiteiten gestandaardiseerd naar EORI, en alle pan-Europese verkeer over organisaties wordt gedaan met EORI, zie bijvoorbeeld deze link (Logius).
Een vaak genoemde alternatief in de gebouwde omgeving is het GLN. Als een organisatie zich zou identificeren met een GLN nummer, is er geen gestandaardiseerde manier om deze te valideren (authenticatie). Met het EORI nummer, in combinatie met eIDAS certificaten, is dit wel mogelijk.
Bovendien wordt EORI ook gebruikt in andere data stelsels. Hierdoor is het DSGO ook interoperabel op gebied van identificatie en authenticatie met deze stelsels.

Als Nederlandse organisatie, kan het EORI-nummer worden samengesteld o.b.v. het RSIN (Rechtspersonen en Samenwerkingsverbanden Informatienummer). Door het RSIN vooraan aan te vullen met '0' tot het nummer 9 cijfers lang is, en vervolgens daarvoor 'NL' toe te voegen, ontstaat het EORI-nummer, zie voorbeeld hieronder.

Organisaties die geen RSIN hebben (zoals Eenmanszaken) kunnen dat hier aanvragen.

⭐ **Voorbeeld:** Wanneer een organisatie een RSIN nummer van 123456 heeft, dan is het EORI nummer van die organisatie NL000123456

Het EORI-nummer wordt ook gebruikt in iSHARE. Gebruik hiervan in het afsprakenstelsel draagt zo bij aan de interoperabiliteit met andere sectoren. Binnen iSHARE wordt elk identificerend kenmerk weergegeven als een URI. Daarom wordt de EU.EORI prefix toegevoegd.

✔️ Partijen MOETEN het EORI-nummer gebruiken met prefix EU.EORI

⭐ **Voorbeeld:** Wanneer een EORI nummer van organisatie NL000123456 is, wordt dat conform iSHARE in berichten opgenomen als URI met prefix EU.EORI, bijv. EU.EORI.NL000123456

**Merk op,** in de context van het DSGO speelt de identificatie van juridische entiteiten een belangrijke rol wanneer deze kan worden geauthenticeerd.

Het EORI nummer, zou voor sommige gevallen niet specifiek kunnen zijn, bijvoorbeeld als het gaat om een specifieke vestiging van een organisatie. Op dit moment is er geen manier om een specifieke identiteit te standaardiseren en authenticeren en is daarom niet opgenomen in het afsprakenstelsel. In de doorontwikkeling van het afsprakenstelsel worden use cases uitgewerkt (zie aanpak). Dit onderwerp zal in die context verder worden onderzocht.

# Identificatie van Personen

Op dit moment is het afsprakenstelsel in ontwikkeling, en zijn nog geen afspraken over de identificatie van personen uitgewerkt. In een toekomstige versie van het afsprakenstelsel zal deze worden ontwikkeld.

# Authenticatie

Authenticatie is het proces waarmee de geldigheid van een geclaimde identiteit van een partij wordt geverifieerd. In het afsprakenstelsel staan afspraken over authenticatie voor de twee soorten interacties, Machine-to-machine en human-to-machine. Onafhankelijk van het type interactie, speelt authenticatie een rol op twee niveaus, op de verbinding tussen partijen, en op datadiensten niveau:

**Authenticatie op transport niveau -** Zodra er wordt gecommuniceerd tussen partijen in het afsprakenstelsel, is het van belang dat de datadienstgebruiker zekerheid heeft over de identiteit van de datadienstaanbieder. Dit voorkomt bijvoorbeeld man-in-the-middle aanvallen waarbij een aanvaller zich probeert voor te doen als de datadienstaanbieder.

**Authenticatie op datadienst niveau -** Wanneer gecommuniceerd wordt over het gebruik van een datadienst, moet worden bepaald of de datadienstgebruiker de juist autorisatie heeft om gebruik te maken van de datadienst. In het komen tot een autorisatie beslissing speelt de authenticiteit van de identiteit van de datadienstgebruiker een belangrijke rol.

Over al deze aspecten zijn in het afsprakenstelsel afspraken over authenticatie opgenomen:

- Authenticatie op Transport Niveau
- Authenticatie op Datadienst Niveau

# Authenticatie op Transport Niveau

In het DSGO, vindt alle communicatie tussen partijen plaats tussen de machines van de partijen. Daarom moet in de verbinding tussen de machines van de partijen authenticatie plaats vinden, zodat er een mate van zekerheid van de identiteit van de machine waarmee gecommuniceerd wordt is. One-way (server only) Transport Layer Security (TLS) wordt gebruikt om de identiteit van datadienstaanbieders te authenticeren.

> Merk op, authenticatie van de datadienstgebruiker gebeurd niet op transport niveau, maar op datadienst niveau via een getekende JWT.

# Authenticatie op Datadienst Niveau

Authenticatie in datadiensten vindt op verschillende manieren plaats, afhankelijk van de type actoren en interacties van partijen die betrokken zijn bij het uitvoeren van de datadienst. Omdat het niet mogelijk is om een mens op dezelfde manier te authenticeren als een machine, zijn voor beide type interacties afspraken opgenomen in het afsprakenstelsel:

- Machine to Machine Authenticatie
- Human to Machine Authenticatie

# Machine to Machine Authenticatie

Wanneer tussen machines wordt gecommuniceerd over het gebruik van een datadienst, moet worden bepaald of de machine van de datadienstgebruiker de juiste autorisatie heeft om gebruik te maken van de datadienst. Bij het bepalen van de autorisatie is een mate van zekerheid van de identificatie van de machine (authenticatie) essentieel. Dit wordt in het afsprakenstelsel mogelijk gemaakt met getekende JSON web tokens (JWT).

# Human to Machine Authenticatie

Voor alle H2M interacties speelt de identificatie van de mens (en authenticatie daarvan) een essentieel onderdeel. Omdat mensen altijd betrokken zijn bij datadiensten middels een machine die namens hun handelen, speelt de Machine-to-machine authenticatie op transport niveau een belangrijke rol. Zie Authenticatie op transport niveau voor meer informatie

De authenticatie van personen op het niveau van een datadienst kan op verschillende manieren worden gerealiseerd. Afhankelijk van de context van de datadienst, kan de nodige mate van zekerheid van de identiteit van de persoon verschillen. Omdat het voldoen aan de eisen van hoge betrouwbaarheidsniveaus kostbaar kan zijn, is het niet gewenst dat alle datadiensten aan dezelfde, hoogste eisen moeten voldoen. Daarom wordt in het afsprakenstelsel gebruik gemaakt van betrouwbaarheidsniveaus.

Op dit moment is het afsprakenstelsel in ontwikkeling, en zijn nog geen afspraken over human to machine authenticatie uitgewerkt. In een toekomstige versie van het afsprakenstelsel zal deze worden ontwikkeld.

# Betrouwbaarheidsniveau (Level of Assurance)

Voor elke datadienst is het nodig om de identiteit van betrokken mensen vast te stellen tot een bepaalde mate van zekerheid: het betrouwbaarheidsniveau. Het gebruik van betrouwbaarheidsniveaus is gebruikelijk bij verschillende diensten, zoals bijvoorbeeld eHerkenning.

:Quotes:

**Bron:** eHerkenning – Betrouwbaarheidsniveaus

EHerkenning heeft 4 betrouwbaarheidsniveaus: EH2, EH2+, EH3 en EH4. De dienstverlener waarbij u inlogt, bepaalt het betrouwbaarheidsniveau van zijn online diensten.

Hoe hoger het betrouwbaarheidsniveau, hoe veiliger en betrouwbaarder de toegang en hoe meer zekerheid een dienstverlener krijgt over met wie hij zaken doet. Eigenschappen van eHerkenning op een hoger niveau:

- meer controlestappen bij uitgifte van een eHerkenningsmiddel
- inloggen met 2-factorauthenticatie

Dit zorgt voor extra zekerheid over de identiteit en bevoegdheid. Zo weet de dienstverlener zeker om welk bedrijf het gaat en of deze persoon bepaalde zaken mag regelen namens dit bedrijf.

Bij het ontwerpen van een datadienst moet een datadienstaanbieder bepalen welk betrouwbaarheidsniveau voor de dienst van toepassing is.

⭐ **Voorbeeld**: Een datadienst die toegang tot data mogelijk maakt kan afhankelijk van de inhoud van de data verschillende betrouwbaarheidsniveaus vereisen:

- Als de data het BIM-model van een gebouw van het ministerie van Defensie betreft dan zal de datadienstaanbieder o.a. een zeer hoge maten van zekerheid nodig hebben in de authenticiteit van de datadienstgebruiker omdat het om zeer gevoelige data gaat.
- Als de data de locaties van alle lantarenpalen in een regio betreft kan de datadienstaanbieder kiezen om een mindere mate van zekerheid in de authenticiteit van de datadienstgebruiker te accepteren als dit de kosten verminderd en gebruikers ervaring versimpeld omdat het om minder gevoelige data gaat.

Elementen die van belang zijn bij het onderwerp van betrouwbaarheidsniveaus zijn bijvoorbeeld:

- Authenticatiemiddelen
- Uitgifte van authenticatiemiddelen
- KYC (Know your Customer)

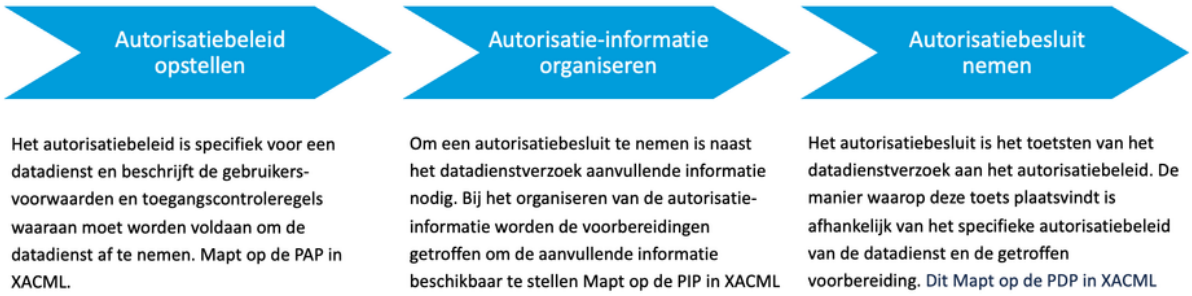
ℹ️ Op dit moment is het afsprakenstelsel in ontwikkeling, en zijn nog geen afspraken over nodige betrouwbaarheidsniveau uitgewerkt. In een toekomstige versie van het afsprakenstelsel zal deze worden ontwikkeld.

# Autorisatie

Autorisatie, identificatie en authenticatie zijn drie essentiële functionaliteiten om een datadienst tussen een datadienstgebruiker en een datadienstaanbieder tot stand te laten komen. Identificatie stelt de identiteit van een partij vast, authenticatie draait om het verifiëren van de identiteit. Vervolgens gaat autorisatie om het vaststellen of de geïdentificeerde partij de rechten heeft en toestemming krijgt om een specifieke actie uit te voeren gegeven de context van de datadienst.

## Aspecten van autorisatie

In het afsprakenstelsel is het onderwerp van autorisatie gesplitst naar het opstellen van autorisatiebeleid, het voorbereiden van autorisatie-informatie en het nemen van een autorisatiebesluit (zie figuur hieronder). Deze verschillende autorisatie aspecten zijn gebaseerd op de XACML standaard voor (online) toegangsbeleid. Gegeven XACML, mapt het autorisatiebeleid op Policy Administration Point (PAP), mapt authorisatie-informatie organiseren op de Policy Information Point (PIP) en het nemen van het autorisatiebesluit op Policy Decision Point (PDP). De Policy Enforcement Point (PEP) wordt geïmplementeerd in de API.




In het DSGO speelt autorisatie een cruciale rol op verschillende punten voor en tijdens het gebruik van datadiensten om gecontroleerd toegang tot data te realiseren

## Complexiteit in autorisatie

Het is de verantwoordelijkheid van een datadienstaanbieder om voor haar datadienst geschikte autorisatie beleid op te stellen en daar besluiten voor te nemen. Afhankelijk van het type datadienst kan dit besluit eenvoudig zijn, of complex en afhankelijke van veel (intern en externe) factoren. Het DSGO biedt datadienstaanbieders keuzes om zo (voor haar specifieke dienst) geschikte autorisatie beslissingen te kunnen nemen. Het afsprakenstelsel standaardiseert voor elke keus een aantal aspecten om de interoperabiliteit van datadiensten in het DSGO te realiseren. De onderstaande indicatieve voorbeelden schetsen een aantal scenario's die gedurende dit hoofdstuk verder worden gebruikt als toelichting.

**Indicatieve voorbeelden:**

*In de voorbeelden loopt de behoefte om complexiteit toe te voegen aan het komen tot een autorisatiebesluit verder op.*

1. Een gemeente (als datadienstaanbieder) heeft een datadienst die de mogelijkheid biedt om een BIM-model te uploaden t.b.v. een vergunningaanvraag. Iedereen die een vergunningaanvraag wil doen, kan deze tool gebruiken (als datadienstgebruiker).
2. Een leverancier (als datadienstaanbieder) heeft een datadienst die productdata (incl. contractdata zoals prijzen) beschikbaar stelt aan afnemers waarmee ze al contracten hebben lopen (als rechthebbende en datadienstgebruikers)
3. Een bouwplaatsbeheerder (als datadienstaanbieder) heeft een datadienst die het mogelijk maakt voor vervoerders (als datadienstgebruiker) om een tijdslot in te plannen voor het afleveren van de goederen. Om dit proces eerlijk te laten verlopen, komen de tijdsloten 48h van tevoren beschikbaar, en is het alleen mogelijk als de vervoerder ook de opdracht heeft gekregen om goederen te leveren.

In de onderliggende pagina's worden de elementen van autorisatie verder gedetailleerd:

- Autorisatiebeleid opstellen
- Autorisatie-informatie organiseren
- Autorisatiebesluit nemen

# Autorisatiebeleid opstellen

Het autorisatiebeleid is specifiek voor elke datadienst en beschrijft de gebruiksvoorwaarden en toegangscontroleregels waaraan moet worden voldaan om de dienst af te mogen nemen. In het autorisatiebeleid ligt vast wie rechthebbenden zijn en wat die rechten inhouden, maar ook of bepaalde kwalificaties en eigenschappen nodig zijn voor toegang tot de datadienst. Ook wordt vastgelegd in welke mate een rechthebbende het recht heeft om (een deel van) zijn rechten te delegeren.

De datadienstaanbieder is verantwoordelijk voor het definiëren van het autorisatiebeleid voor haar datadienst. De datadienstaanbieder bezit en beheert zelf de informatie over rechten, inclusief tot welke (delen van) datadiensten rechthebbende gerechtigd zijn. De manier waarop de datadienstaanbieder het autorisatiebeleid opstelt is niet gedefinieerd in het afsprakenstelsel. De datadienstdefinitie bevat de informatie over het autorisatiebeleid zodat het op een gestandaardiseerde manier kan worden gecommuniceerd met (potentiële) datadienstgebruiker.

✔️ Datadienstaanbieders MOETEN het autorisatiebeleid bepalen voor elke datadienst

✔️ Datadienstaanbieders MOETEN hun autorisatiebeleid vastleggen in de toegangscontroleregels van de datadienstdefinitie

## Complexiteit in autorisatiebeleid

Afhankelijk van het type datadienst zit er veel variatie in het autorisatiebeleid

⭐ **Indicatieve voorbeelden:**

*In de voorbeelden loopt de behoefte om complexiteit toe te voegen aan het komen tot een autorisatiebesluit. Deze voorbeelden zijn op de Autorisatie pagina geïntroduceerd.*

1. Een gemeente (als datadienstaanbieder) heeft een datadienst die de mogelijkheid biedt om een BIM-model te uploaden t.b.v. een vergunningaanvraag. Iedereen die een vergunningaanvraag wil doen, kan deze tool gebruiken (als datadienstgebruiker). In het autorisatiebeleid staat bijvoorbeeld opgenomen:
   - Iedereen mag van deze datadienst gebruik maken.
2. Een leverancier (als datadienstaanbieder) heeft een datadienst die productdata (incl. contractdata zoals prijzen) beschikbaar stelt aan afnemers waarmee ze al contracten hebben lopen (als rechthebbende en datadienstgebruikers). In het autorisatiebeleid staat opgenomen bijvoorbeeld opgenomen:
   - Afnemers mogen enkel bij hun eigen contractdata.
   - Afnemers mogen hun rechten aan derden delegeren.
3. Een bouwplaatsbeheerder (als datadienstaanbieder) heeft een datadienst die het mogelijk maakt voor vervoerders (als datadienstgebruiker) om een tijdslot in te plannen voor het afleveren van de goederen. Om dit proces eerlijk te laten verlopen, komen de tijdsloten 48h van tevoren beschikbaar, en is het alleen mogelijk als de vervoerder ook de opdracht heeft gekregen om goederen te leveren. In het autorisatiebeleid staat opgenomen bijvoorbeeld opgenomen:
   - De specifieke data pas 48 uur voor de geplande bezorging beschikbaar is
   - Enkel partijen met een geldende opdracht mogen gebruik maken van de datadienst.

# Autorisatie-informatie organiseren

Om een autorisatiebesluit mogelijk te maken bij een datadienstverzoek, is naast het verzoek aanvullende informatie nodig. In het autorisatiebesluit wordt deze informatie omtrent het verzoek getoetst tegen het autorisatiebeleid. In het organiseren van autorisatie-informatie worden de voorbereidingen getroffen om deze informatie beschikbaar te stellen bij het maken van het autorisatiebesluit. Afhankelijk van het autorisatiebeleid kan het organiseren van autorisatie-informatie over verschillende type informatie gaan, daarmee zijn alle type autorisatie-informatie optioneel voor gebruik door datadienstaanbieders. Bijvoorbeeld het uitgeven van bepaalde kwalificaties en eigenschappen die bij het datadienstverzoek nodig zijn, het registeren van gedelegeerde rechten of het gebruik van een access token.

## Access Token

**Doel:** Acces tokens maken het mogelijk voor datadienstaanbieders om de functionaliteit van autorisatie onafhankelijk uit te voeren van de datadienst. Dit biedt een schaalbare oplossing die in de praktijk vaak voorkomt.

Een access token dienst als bewijs dat een partij de rechten heeft om een datadienstverzoek te sturen. In het afsprakenstelsel wordt het OAuth 2.0 protocol gebruikt om access tokens op te halen. Veel huidige toepassingen verwachten het gebruik van OAuth 2.0 access tokens bij het aanroepen van een dienst. Een access token maakt het mogelijk voor de gebruiker om eenmalig te autoriseren voor de aanvraag van meerdere diensten. In het DSGO wordt in bij aanvraag van een access token de authenticiteit van de aanvrager vastgelegd middels getekende JWTs.

✔️ Als datadienstaanbieders gebruik maken van een access token dan MOET dit worden gedaan volgens het afsprakenstelsel

In Access token wordt het onderwerp van access tokens verder gedetailleerd.

## Delegatie

**Doel:** Het ondersteunen van delegatie door datadienstaanbieders stelt de rechthebbende in staat om haar recht op toegang tot (de bewerking van) data over te dragen.

Delegatie is het overdragen van een bevoegdheid, van de rechthebbende, aan een ander die vervolgens die bevoegdheid kan gebruiken. De datadienstaanbieder kan het mogelijk maken om rechten te delegeren  om de soevereiniteit van de rechthebbende te bevorderen of functionaliteiten breder aan te bieden. Het delegeren van rechten binnen het DSGO volgt de doelstelling van het DSGO om partijen in staat te stellen om data vanuit de bron beschikbaar te stellen. Dit zorgt ervoor dat in een federatief ecosysteem voor datadelen er geen onnodige data replicatie plaatsvindt waar data telkens moet worden doorgestuurd. Rechthebbende kunnen rechten delegeren aan andere partijen zodat data zij data direct van de bron kunnen ophalen. Echter, het delegeren van rechten is niet altijd relevant of mogelijk.

✔️ Datadienstaanbieders ZOUDEN het voor de rechthebbende mogelijk MOETEN maken haar rechten over data te delegeren

ℹ️ **Merk op,** wanneer een datadienstaanbieder zelfstandig de enkele rechthebbende is over data die in een datadienst beschikbaar wordt gesteld, kan deze bepalen dat het delegeren van rechten niet mogelijk is.

In het DSGO zijn er drie manieren waarop delegaties kunnen worden geregistreerd en beheert, zodat deze als informatie kunnen worden gebruikt door de datadienstaanbieder bij het maken een autorisatiebesluit.

1. **De rechthebbende beheert zelf delegaties.** De rechthebbende heeft (in afstemming met de datadienstaanbieder) bepaald dat de rechthebbende voor elk verzoek om een datadienst toestemming moet geven.
2. **De rechthebbende registreert zijn delegaties bij de datadienstaanbieder.** De rechthebbende bepaalt en deelt haar delegatieregels op basis waarvan de datadienstaanbieder autonoom een autorisatiebesluit kan nemen.

3. **De rechthebbende registreert zijn delegaties bij een onafhankelijk autorisatieregister.** De rechthebbende heeft voordat een datadienstverzoek plaatsvindt haar delegaties geregistreerd in een onafhankelijk autorisatieregister.

In Delegaties wordt het delegeren van rechten verder toegelicht.

## Kwalificaties en eigenschappen

**Doel:** Kwalificaties en eigenschappen worden gebruikt zodat een datadienstaanbieder modulair kan bepalen onder welke voorwaarden een partij toegang krijgt tot een datadienst en dit mogelijk aan te brengen in delegaties.

In het autorisatiebeleid kan zijn bepaald dat voor het gebruik van een datadienst kan de datadienstaanbieder bepalen dat datadienstgebruikers kwalificaties en eigenschappen moeten hebben. Bijvoorbeeld dat de partij ISO27001 gecertificeerd is, een BRL6000-21/00 certificering heeft voor het installeren van een warmtepomp, of lid is van Techniek Nederland. In de voorbereiding voor het gebruik van de datadienst moeten de nodige kwalificaties en eigenschappen worden behaald, geregistreerd en klaar gemaakt om beschikbaar te stellen aan de datadienstaanbieder voor controle bij het nemen van een autorisatiebesluit.

✔️ Als datadienstaanbieders gebruik maken van kwalificaties en eigenschappen dan MOET dit worden gedaan volgens het afsprakenstelsel

**Merk op,** het afsprakenstelsel is in ontwikkeling. In een volgende versie van het afsprakenstelsel zal het mechanisme voor het organiseren van kwalificaties en eigenschappen worden beschreven.

## Complexiteit in autorisatie-informatie

Afhankelijk van het type datadienst zit er veel variatie in de voorbereiding van autorisatie-informatie

⭐ **Indicatieve voorbeelden:**

*In de voorbeelden loopt de behoefte om complexiteit toe te voegen aan het komen tot een autorisatiebesluit. Deze voorbeelden zijn op de Autorisatie pagina geïntroduceerd.*

1. Een gemeente (als datadienstaanbieder) heeft een datadienst die de mogelijkheid biedt om een BIM-model te uploaden t.b.v. een vergunningaanvraag. Iedereen die een vergunningaanvraag wil doen, kan deze tool gebruiken (als datadienstgebruiker). In dit geval is geen additionele autorisatie-informatie nodig.
2. Een leverancier (als datadienstaanbieder) heeft een datadienst die productdata (incl. contractdata zoals prijzen) beschikbaar stelt aan afnemers waarmee ze al contracten hebben lopen (als rechthebbende en datadienstgebruikers). In dit geval kan de volgende autorisatie-informatie relevant zijn:
   - Een access token van de afnemer als bewijs van authenticiteit
   - Delegatie informatie zodat de afnemers rechten aan derden kunnen delegeren
3. Een bouwplaatsbeheerder (als datadienstaanbieder) heeft een datadienst die het mogelijk maakt voor vervoerders (als datadienstgebruiker) om een tijdslot in te plannen voor het afleveren van de goederen. In dit geval kan de volgende autorisatie-informatie relevant zijn:
   - Delegatie informatie zodat de vervoerder rechten aan de chauffeur kan delegeren
   - Kwalificaties van de chauffeur om deze te valideren
   - Een access token van de vervoerders als bewijs van authenticiteit
   - Bewijs dat er daadwerkelijk een opdracht is tussen de bouwplaatsbeheerder en de vervoerders

# Access token

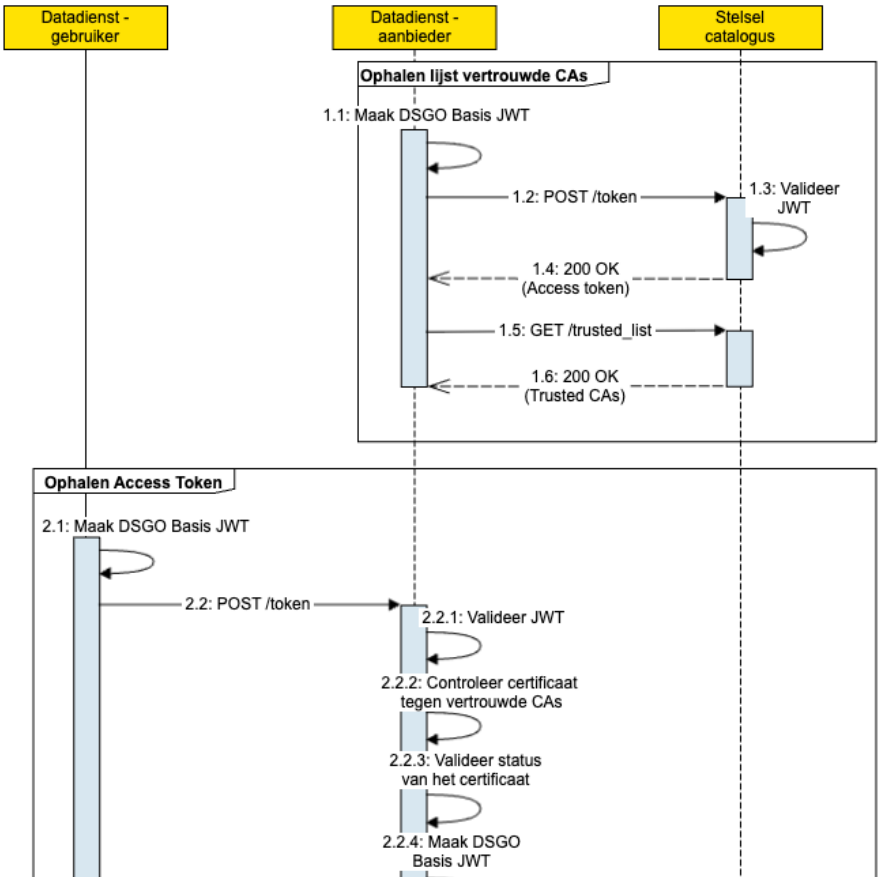
Bij het aanbieden van datadiensten is autorisatie een essentieel onderdeel. Een (potentiële) datadienstgebruiker moet aan tonen dat ze geautoriseerd zijn om gebruik te maken van een datadienst van een datadienstaanbieder. Een datadienstaanbieder kan ervoor kiezen om hier access tokens voor te gebruiken. Access tokens maken het mogelijk voor datadienstaanbieders om de functionaliteit van autorisatie onafhankelijk uit te voeren van de datadienst. Voor de gebruiker maakt een access token het mogelijk om eenmalig te autoriseren voor de aanvraag van meerdere diensten. Daarmee biedt is het concept van een access token een schaalbare oplossing die in de praktijk vaak voorkomt.

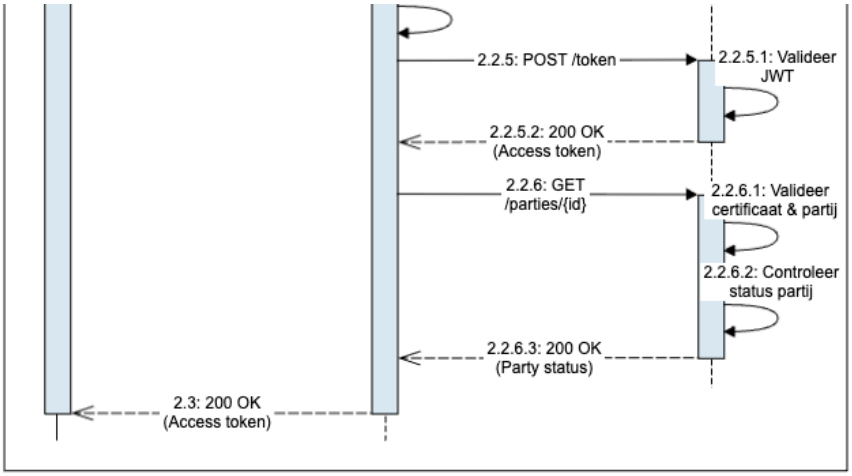
In het DSGO wordt het OAuth 2.0 protocol gebruikt om access tokens op te halen. Voor machine-to-machine (M2M) interacties kan een access token verkregen worden via een /token endpoint, volgens OAuth 2.0 client credentials. Bij het aanvragen van de access token wordt de identifiteit van de aanvrager geauthenticeerd. Hiervoor wordt een getekende JWT gebruikt volgens de OAuth 2.0 JWT bearer profile. Tevens wordt bij de aanvraag van een access token gecontroleerd wat de status van de aanvrager is binnen het DSGO (zie hieronder).

✔ Als partijen gebruik willen maken van een access token dan, MOETEN ze deze beschikbaar stellen via een /token endpoint

In de onderstaande figuur staat het interactiemodel beschreven waarmee een access token kan worden opgehaald. Dit interactie model bestaat uit drie kern elementen om een access token te kunnen ophalen: het ophalen van de lijst van vertrouwde certificaatautoriteiten, het valideren van het certificaat, en het controle van de status van de partij. Dit interactiemodel is volledig inlijn met de authenticatie flow van iSHARE. Voor meer details over de werking van de specifieke endpoints en de implementatie hiervan zie API specifications.

ℹ **Merk op,** in dit voorbeeld interactiemodel haalt een datadienstgebruiker een access token op bij een datadienstaanbieder. Elke rol in het DSGO kan deze rollen invullen afhankelijk van de situatie. Bijvoorbeeld een datadienstaanbieder die een token bij een marktvoorziening.






## Ophalen lijst van vertrouwde Certificaatautoriteit

Elk verzoek voor een access token in het DSGO moet altijd ondertekend zijn door een certificaat dat is uitgegeven door een certificaatautoriteit op de vertrouwde lijst van DSGO. Elke deelnemer kan de vertrouwde lijst opvragen bij de `/trusted_list` endpoint van de stelselcatalogus, zie /trusted_list voor meer details.

## Certificaat validatie

Een verzoek voor een access token bevat een getekende Basis JWT om informatie over de identiteit van de aanvrager te communiceren. Wanneer een partij een verzoek ontvangt voor een access token, moet de ontvangende partij het certificaat waarmee deze is getekend valideren.

- ✔️ Partijen MOETEN verifiëren dat het certificaat waarmee de Basis JWT is getekend uitgegeven en ondertekend is door een certificaatautoriteit op de vertrouwde lijst van DSGO
- ✔️ Partijen MOETEN verifiëren dat het certificaat waarmee Basis JWT is getekend valide is

## Controle status partij

Nadat het certificaat van de aanvrager is gecontroleerd, moet de identiteit van de partij en haar status binnen het DSGO gecontroleerd worden. De identiteit van de partij wordt geauthenticeerd door de identiteit vanuit het certificaat te vergelijken met die in het verzoek om een access token, voor meer informatie zie /token endpoint. De status van een partij binnen het DSGO kan worden gecontroleerd bij de `/parties` endpoint van de stelselcatalogus, zie /parties voor meer details.

- ✔️ Partijen MOETEN bij elk verzoek om een access token, de identiteit van de aanvrager authenticeren door de identiteit uit het certificaat te vergelijken met die uit het access token verzoek. Indien deze niet matchen met elkaar, MOETEN het verzoek worden afgewezen.
- ✔️ Partijen MOETEN bij een access token verzoek de status van een partij binnen het DSGO verifiëren bij de stelselcatalogus

# Delegaties

Delegatie is het overdragen van een bevoegdheid, van de rechthebbende, aan een ander die vervolgens die bevoegdheid kan gebruiken. Wanneer een datadienstaanbieder het in een datadienst mogelijk maakt voor een rechthebbende om haar rechten te delegeren, moeten de door de rechthebbende gedelegeerde rechten van tevoren zijn geregistreerd. Wanneer daarna een gedelegeerde datadienstgebruiker een datadienstverzoek verstuurt moet de datadienstaanbieder het delegatiebewijs beschikbaar krijgen of op basis van de ontvangen informatie zelf een autorisatiebesluit kunnen nemen.

## Registratie van delegaties

Gedelegeerde rechten kunnen op drie verschillende plekken geregistreerd worden. De meest geschikte optie voor het registreren van delegaties is afhankelijk van de situatie, en behoeftes van betrokken partijen. Bovendien brengen de drie opties verschillende implementatielasten mee voor verschillende rollen en verschillende interactiemodellen. De drie opties zijn:

1. De rechthebbende beheert zelf delegaties
2. De rechthebbende registreert haar delegaties bij de datadienstaanbieder
3. De rechthebbende registreert haar delegaties bij een onafhankelijk autorisatieregister

De datadienstaanbieder is verantwoordelijk voor het vaststellen waar delegaties geregistreerd kunnen worden in haar datadienst De rechthebbende heeft binnen de aangeboden opties keuze over waar ze haar delegaties geregistreerd.

✔ Als gedelegeerde datadienstgebruikers een datadienst kunnen afnemen MOETEN datadienstaanbieders vaststellen waar delegaties geregistreerd mogen worden

✔ Als de rechthebbende gebruik wil maken van de mogelijkheid om haar rechten te delegeren dan MOET de rechthebbende binnen de opties aangeboden in een datadienst bepalen waar haar delegaties geregistreerd worden

### De rechthebbende beheert zelf delegaties

Wanneer de rechthebbende haar delegaties zelf beheert moet de rechthebbende elke gedelegeerde datadienstgebruiker toestemming geven voordat deze een datadienstverzoek kan sturen. Dit is geschikt bij datadiensten met zeer waardevolle data waar de rechthebbende volledige controle over wil hebben.

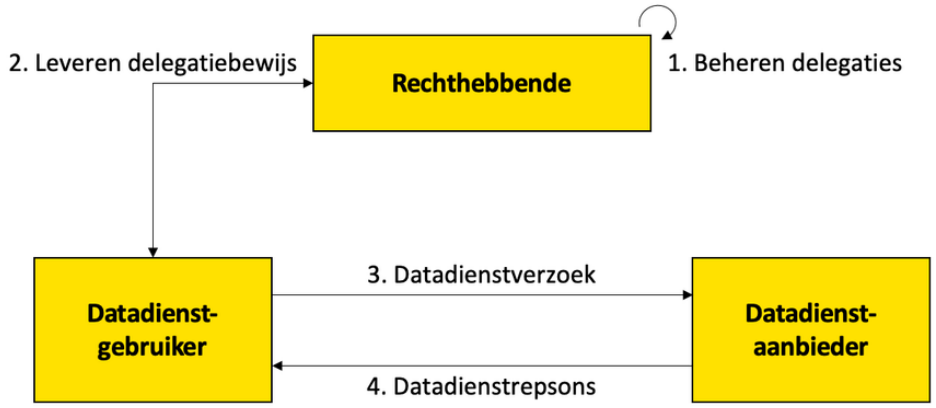
✔ Als een datadienstaanbieder de mogelijkheid biedt voor de rechthebbende om zelf haar delegaties te beheren dan MOET dit worden gedaan volgens het afsprakenstelsel

**Merk op,** het afsprakenstelsel is in ontwikkeling. In een volgende versie van het afsprakenstelsel zal het mechanisme voor rechthebbende om zelf delegaties te beheren en beschikbaar te stellen voor gebruik in een datadienst worden toegevoegd. Dit zal worden gedaan op basis van iSHARE.

#### Interactiemodel

Om dit mogelijk te maken, moet de rechthebbende een delegatiebewijs leveren aan de datadienstgebruikers aan wie zij haar rechten overdraagt. Daarvoor moet de rechthebbende haar systemen zo inrichten dat ze haar eigen delegaties kan registreren en een delegatiebewijs kan leveren aan datadienstgebruikers die het aanvragen (zie het interactiemodel in het figuur hieronder). Dit heeft een implementatie implicatie voor de rechthebbende en de datadienstgebruiker.

**Merk op,** Op dit moment is gekozen voor dit interactiemodel omdat het federatief ecosysteem voor datadelen (DSGO) nog in ontwikkeling is, en de implementatielast wordt gelegd bij de partijen die er waarde uit ervaren. Andere interactiemodellen kunnen deze functionaliteit mogelijk te maken, waarbij de implementatie last bij de datadienstaanbieder ligt. In de toekomst, in een volwassen DSGO, is dit wellicht gewenst, en kan dit worden herzien.




Het interactiemodel bij een datadienst wanneer de rechthebbende zelf haar delegaties beheert

| # | Acties | Omschrijving |
|---|---|---|
| 1 | Beheren delegaties | De rechthebbende bepaalt zelf aan wie zij haar rechten overdraagt |
| 2 | Leveren delegatiebewijs | De rechthebbende levert een delegatiebewijs aan de datadienstgebruikers aan wie ze haar rechten overdraagt |
| 3 | Datadienst-verzoek | De gedelegeerde datadienstgebruiker voegt het delegatiebewijs toe in de datadienstverzoek als autorisatie-informatie |
| 4 | Datadienst-respons | De datadienstaanbieder valideert het ontvangen delegatiebewijs, en gebruikt deze informatie om te komen tot een autorisatiebesluit. Bij een positief autorisatiebesluit wordt de datadienst uitgevoerd |

## De rechthebbende registreert haar delegaties bij de datadienstaanbieder

Wanneer delegaties geregistreerd zijn bij de datadienstaanbieder bepaalt en deelt de rechthebbende de delegatieregels met de datadienstaanbieder op basis waarvan de datadienstaanbieder autonoom een gedelegeerde datadienstgebruiker toestemming kan geven. Dit is geschikt in het geval de datadienstaanbieder over de software beschikt welke technische integratie mogelijk maakt tussen de rechthebbende en de datadienstaanbieder.

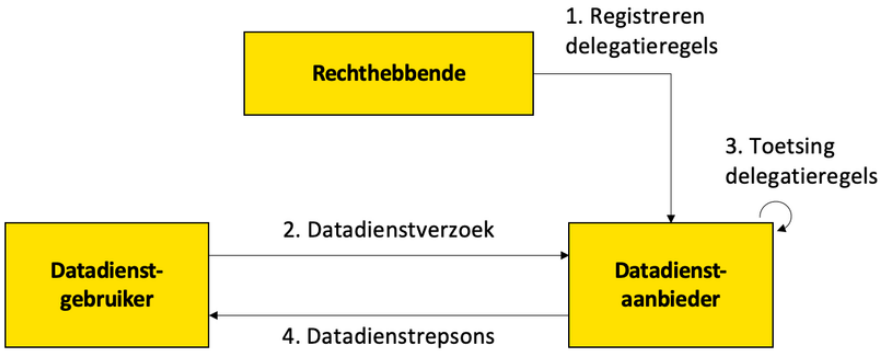
✔ Als een datadienstaanbieder de mogelijkheid biedt voor rechthebbende om haar delegaties te registreren bij de datadienstaanbieder dan MOET de datadienstaanbieder dit mogelijk maken voor de rechthebbende

**Merk op,** het afsprakenstelsel definieert niet hoe de registratie van delegaties bij de datadienstaanbieder moet plaatsvinden. Dit is omdat bij deze delegatie registratie keuze geen afhankelijkheden liggen bij andere partijen, en daarmee de implementatie hiervan geen impact heeft op interoperabiliteit in het DSGO.

### Interactiemodel

In het geval de datadienstaanbieder delegaties beheert moet zij bij ieder datadienstverzoek in staat zijn de informatie in dat verzoek te toetsen tegen de delegatieregels van de rechthebbende om op basis daarvan een besluit te nemen. Hiervoor moet de datadienstaanbieder

haar systemen en/of processen zo inrichten dat een rechthebbende haar delegatieregels kan registeren, en deze worden getoetst bij elk datadienstverzoek (zie het interactiemodel in het figuur hieronder). Dit heeft een implementatie implicatie voor de datadienstaanbieder.




Het interactiemodel bij een datadienst wanneer delegaties geregistreerd zijn bij de datadienstaanbieder

| # | Acties | Omschrijving |
|---|---|---|
| 1 | Registreren delegatieregels | De rechthebbende registreert haar delegatieregels bij de datadienstaanbieder |
| 2 | Datadienst-verzoek | De gedelegeerde datadienstgebruiker stuurt een datadienstverzoek met daarin autorisatie-informatie die getoetst kan worden tegen de delegatieregels |
| 3 | Toetsing delegatieregels | De datadienstaanbieder toetst de autorisatie-informatie in het datadienstverzoek tegen de delegatieregels en neemt op basis daarvan een autorisatiebesluit |
| 4 | Datadienst-respons | Bij een positief autorisatiebesluit wordt de datadienst uitgevoerd |

## De rechthebbende registreert haar delegaties bij een onafhankelijk autorisatieregister

Wanneer de rechthebbende haar delegaties registreert bij een autorisatieregister vraagt de datadienstaanbieder bij een datadienstverzoek van een gedelegeerde datadienstgebruiker het delegatiebewijs op bij het autorisatieregister. Dit is geschikt in het geval waar schaalbaarheid belangrijk is. Een autorisatieregister kan het beheer van een groot aantal delegaties op haar nemen.

✔ Als een datadienstaanbieder de mogelijkheid biedt voor rechthebbende om haar delegaties te registreren bij een autorisatieregister dan MOET dit worden gedaan volgens het afsprakenstelsel

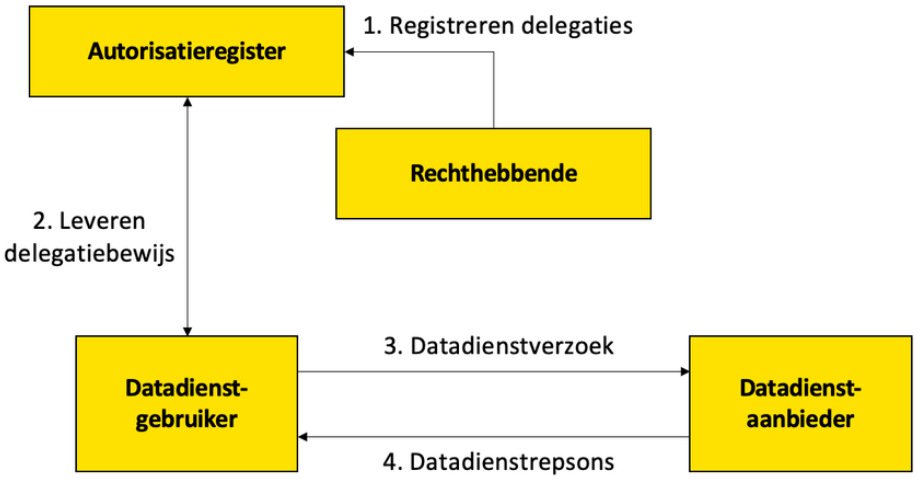
**Merk op,** het afsprakenstelsel is in ontwikkeling. In een volgende versie van het afsprakenstelsel zal het mechanisme voor rechthebbende om delegaties te beheren in een autorisatieregister voor gebruik in een datadienst worden toegevoegd. Dit zal worden gedaan op basis van iSHARE.

### Interactiemodel

Als de rechthebbende haar delegaties geregistreerd bij een autorisatieregister moet de datadienstgebruiker voor het versturen van een datadienstverzoek delegatiebewijs ophalen bij het autorisatie register. De datadienstgebruiker moet daarvoor een koppeling ontwikkelen die aansluit op de systemen van het autorisatieregister (zie het interactiemodel in het figuur hieronder). Dit heeft een implementatie implicatie voor de rechthebbende en datadienstaanbieder.

**Merk op,** Op dit moment is gekozen voor dit interactiemodel omdat het federatief ecosysteem voor datadelen (DSGO) nog in ontwikkeling is, en de implementatielast wordt gelegd bij de partijen die er waarde uit ervaren. Andere interactiemodellen kunnen

deze functionaliteit mogelijk te maken, waarbij de implementatie last bij de datadienstaanbieder ligt. In de toekomst, in een volwassen DSGO, is dit wellicht gewenst, en kan dit worden herzien.



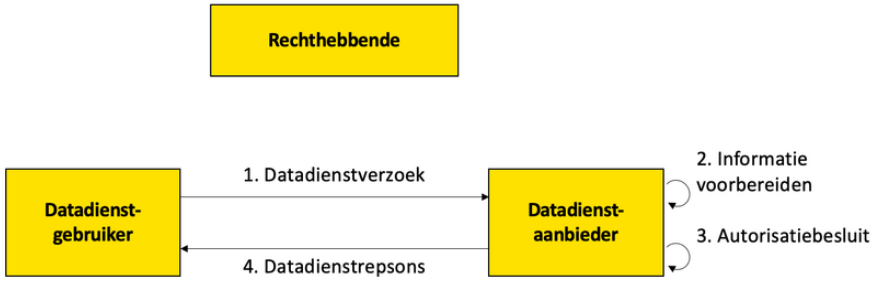

Het interactiemodel bij een datadienst wanneer delegaties geregistreerd zijn bij een onafhankelijk autorisatieregister

| # | Acties | Omschrijving |
|---|---|---|
| 1 | Registreren delegaties | De rechthebbende registreert haar delegatieregels bij een autorisatieregister |
| 2 | Opvragen delegatiebewijs | Het autorisatieregister levert een delegatiebewijs aan de datadienstgebruikers aan wie de rechten van de rechthebbende zijn overgedragen |
| 3 | Datadienst-verzoek | De gedelegeerde datadienstgebruiker voegt het delegatiebewijs toe in de datadienstverzoek als autorisatie-informatie |
| 4 | Datadienst-respons | De datadienstaanbieder valideert het ontvangen delegatiebewijs, en gebruikt deze informatie om te komen tot een autorisatiebesluit. Bij een positief autorisatiebesluit wordt de datadienst uitgevoerd |

# Autorisatiebesluit nemen

Een (potentiële) datadienstgebruiker doet een datadienstverzoek bij een datadienstaanbieder. Dit verzoek wordt door de datadienstaanbieder getoetst aan het autorisatiebeleid, als autorisatiebesluit, om te controleren of de datadienstgebruiker toegang krijgt tot de datadienst. De manier waarop deze toets plaatsvindt, is afhankelijk van de specifieke datadienst autorisatiebeleid en de voorbereiding die hiervoor is getroffen.

In de figuur hieronder wordt het interactiemodel weergegeven hoe een autorisatiebesluit tot stand komt.




Het interactiemodel om tot een autorisatiebesluit te komen

## 1. Datadienstverzoek

De datadienstgebruiker dient een verzoek tot het gebruik van een datadienst in bij de datadienstaanbieder. Het datadienstverzoek is niet gedefinieerd in het afsprakenstelsel, omdat dit afhankelijk is van de datadienst zelf (zie deze pagina voor een voorbeeld datadienst). Het datadienstverzoek kan informatie bevatten die van belang is voor het autorisatiebesluit.

## 2. Informatie voorbereiden

De datadienstaanbieder haalt informatie op uit het datadienstverzoek, en eventueel extra informatie die voor het datadienstverzoek is georganiseerd die nodig is bij het komen tot een autorisatiebesluit. De nodige informatie is afhankelijk van het autorisatiebeleid en de getroffen voorbereidingen. Afhankelijk van de datadienst kan dit informatie bevatten over (o.a.) kwalificaties en eigenschappen, delegatie of een access token.

## 3. Autorisatiebesluit

Om een autorisatiebesluit te nemen zou de datadienstaanbieder de informatie betreffend het datadienstverzoek moeten houden tegen het opgestelde autorisatiebeleid. De datadienstaanbieder is verantwoordelijk om de juiste informatie te controleren bij het nemen van een autorisatiebesluit. Er kunnen redenen ontstaan voor het afwijken van autorisatiebeleid, zelfs wanneer alle nodige autorisatie-informatie correct is voorbereid, bijvoorbeeld het gebruik van een blacklist. In een geval waar dit voorkomt, is het de verwachting dat de datadienstaanbieder haar besluit kan onderbouwen en communiceren aan de datadienstaanbieder indien nodig.

✔️ Datadienstaanbieders ZOUDEN MOETEN handelen naar haar autorisatiebeleid

## 4. Datadienstrespons

Afhankelijk van het autorisatiebesluit voert de datadienstaanbieder een response uit en wordt dit gecommuniceerd met de datadienstgebruiker via de methode zoals gespecificeerd in de datadienst.

# Informatiebeveiliging

Met behulp van maatregelen op het gebied van informatiebeveiliging beoogt het DSGO de risico's die bij het gebruik van het DSGO optreden wanneer er data wordt gedeeld zoveel mogelijk te mitigeren. Deze informatiebeveiligingsrisico's hebben betrekking op het volledige end-to-end proces van datadelen, van registratie tot uitwisseling en gebruik en (ver) daarna. Over de volgende onderwerpen zijn afspraken gemaakt:

- Transport layer security
- JSON Web Tokens (JWT)
- Onweerlegbaarheid

**Merk op**, de lijst met onderwerpen wordt in volgende versies van het afsprakenstelsel uitgebreid indien nodig.

## Risicomanagement

Naast de opgestelde afspraken is elke partij verantwoordelijk haar eigen risico's rondom datadelen in kaart te brengen door middel van een risicoanalyse. Afhankelijk van deze risicoanalyse kan de partij mitigerende maatregelen nemen. Deze maatregelen zijn bijvoorbeeld technisch, operationeel of juridisch van aard.

✔ Partijen ZOUDEN een risicoanalyse uit MOETEN voeren

✔ Partijen ZOUDEN passende informatiebeveiligingsmaatregelen MOETEN nemen

✔ Partijen ZOUDEN andere partijen waarmee wordt samengewerkt MOETEN aansporen passende informatiebeveiligingsmaatregelen te nemen

# Transport layer security

## Transport Layer Security (TLS)

Het afsprakenstelsel maakt gebruik van Transport Layer Security (TLS) om de vertrouwelijkheid van informatie van communicatie over HTTP te waarborgen. Wanneer HTTP communicatie beveiligd is volgens het TLS protocol is sprake van HTTPS (HypterText Transfer Protocol Secure). Hiermee is het afsprakenstelsel in lijn met de API strategie voor de Nederlandse Overheid, het iSHARE scheme en het Data Sharing Coalition Use Case Implementation Guide die gebaseerd zijn op deze zelfde standaarden.

:Quotes:

**Bron:** API strategie voor de Nederlandse Overheid - API Beveiliging

API's zijn vanaf elke locatie vanaf het internet te benaderen. Om uitgewisselde informatie af te schermen wordt altijd gebruik gemaakt van een versleutelde verbinding op basis van TLS. Geen uitzonderingen, dus overal en altijd.

De meest recente en wenselijke versie van TLS is v1.3, en is beschreven in RFC 8446. TLS v1.2 is een vaak voorkomende implementatie van TLS, en is beschreven in RFC 5246. Om interoperabiliteit tussen systemen te garanderen kan in het DSGO altijd worden teruggevallen op TLS v1.2.

✔️ Partijen MOETEN API endpoints beveiligen met minimaal TLS v1.2

✔️ Partijen ZOUDEN API endpoints MOETEN beveiligen met TLS v1.3

✔️ Partijen MOETEN API verzoeken die niet beveiligd zijn met TLS v1.2 of TLS v1.3 afwijzen

✔️ Partijen MOETEN voor alle machine-to-machine interacties gebruik maken van one-way (server only) TLS

✔️ Partijen MOETEN voor alle human-to-machine interacties gebruik maken van one-way (server only) TLS

✔️ Partijen MOETEN bij toepassing van het TLS protocol certificaten gebruiken met een minimale sleutellengte van 2048 bits en maximale geldigheid van twee jaar

## TLS  Certificaten

Het afsprakenstelsel maakt gebruik van QWACs (Qualified Website Authentication Certificates) in TLS om de identiteit van webservers te authenticeren en de vertrouwelijkheid, integriteit en authenticiteit van communicatie tussen partijen mogelijk te maken. QWACs worden in lijn met de eIDAS regulering uitgegeven door gekwalificeerde vertrouwensdienstverleners op de List of Trusted Lists (LOTL).

:Quotes:

**Bron:** European Parlaimant - Qualified certificates for website authentication

**What is a qualified certificate for website authentication (QWAC)?**

A QWAC is a website authentication certificate governed by the eIDAS Regulation. Each QWAC contains information about the entities issuing and receiving the certificate, as well as information about the certificate itself. QWACs are issued by qualified trust service providers (QTSPs) as defined in the eIDAS regulation. QWACs are used beyond websites as they authenticate the connection and the identity of the entity or person in control of the connection.

✔️ Partijen MOETEN QWACS als certificaat gebruiken voor het one-way (server only) TLS protocol

✔️ Partijen MOETEN alle root certificaten voor QWACs van CAs op de EU/EEA List of Trusted Lists (LOTL) en PKIO accepteren

# JSON Web Tokens (JWT)

Het afsprakenstelsel maakt gebruik van JSON Web Tokens (JWT) voor de communicatie van informatie tussen partijen in de context van een datadienst. JWT (JSON Web Token) is een open standaard die een compacte en op zichzelf staande manier definieert om informatie veilig te verzenden tussen partijen door een JSON-object. In het afsprakenstelsel worden JWTs digitaal getekend (als JWS volgens RFC 7515), waardoor informatie in de JWTs kan worden vertrouwd.

Op deze pagina worden de generieke afspraken die gelden voor het gebruik van JWT vastgelegd, deze zijn in lijn met de API strategie voor de Nederlandse Overheid, het iSHARE scheme en het Data Sharing Coalition Use Case Implementation Guide, waarin deze standaard ook gebruikt wordt.

Het DSGO definieert twee soorten JWTs die voor verschillende doeleindes worden gebruikt. Een Basis (Basic) JWT om informatie over de identiteit van een partij te communiceren, en een Geavanceerde (Advanced) JWT die boven op de Basis JWT additionele informatie bevat (zoals beschreven in ETSI TS 119 182-1) om de onweerlegbaarheid van content waar in de JWT naar wordt verwezen te garanderen.

## JWT Signing (JWS)

Informatie bevat in de JSON-object kan worden geverifieerd en vertrouwd omdat deze digitaal zijn ondertekend. JWTs kunnen worden ondertekend met behulp van de JSON Web Signature (JWS) standaard (volgens RFC 7515) om onweerlegbaarheid van deze claims te garanderen.

✔️ Partijen MOETEN alle JWTs ondertekenen als een JSON Web Signature (JWS) zoals beschreven in RFC 7515

✔️ Partijen MOETEN alle getekende Geavanceerde JWTs formatteren volgens JWS Compact Serialisation

## JWT Header

✔️ Partijen MOETEN het RS256 algoritme gebruiken bij het ondertekenen van alle JWTs

✔️ Partijen MOETEN in Basis JWTs de parameters gebruiken  als JWT headers zoals opgesteld in de onderstaande tabel

✔️ Partijen MOETEN in Geavanceerde JWTs de parameters gebruiken als JWT headers zoals opgesteld in de onderstaande tabel

✔️ Partijen MOGEN in alle JWTs andere parameters NIET als JWT headers gebruiken

| **JWT headers** | | | **Beschrijving** |
|---|---|---|---|
| **van toepassing voor:** | Basis JWT | Geavanceerde JWT | |
| `alg` | Vereist | Vereist | Als beschreven in RFC 7515, MOET ingevuld worden als `“RS256"` |
| `b64` | Niet aanwezig | Vereist | Als beschreven in RFC 7797, MOET ingevuld worden als `false` |
| `crit` | Niet aanwezig | Vereist | Als beschreven in RFC 7515, MOET ingevuld worden als `["sigT","sigD","b64"]` |

| | | | |
|---|---|---|---|
| `sigT` | Niet aanwezig | Vereist | Als beschreven in ETSI TS 119 182-1, MOET ingevuld worden als het tijdstip dat de tekening is gezet, geformatteerd volgens UTC |
| `sigD` | Niet aanwezig | Vereist | Als beschreven in ETSI TS 119 182-1, zie tabel hieronder voor meer informatie. |
| `typ` | Vereist | Vereist | Als beschreven in RFC 7515, MOET ingevuld worden als `"JWT"` voor een Basis JWT en `"JOSE"` voor een Geavanceerde JWT |
| `x5c` | Vereist | Vereist | Als beschreven in RFC7523, zal de QSEAL voor de ondertekening bevatten |

De `sigT` header is toegevoegd in de Geavanceerde JWT zodat deze kan worden vergeleken met de HTTP-transactie tijd om het risico van “replay attacks” te mitigeren. Verder, omdat de tijd van tekenen wordt geaccepteerd door beide partijen kan het worden gebruikt als een tijd van de transactie om de onweerlegbaarheid te ondersteunen.

De `sigD` header is toegevoegd in de Geavanceerde JWT om een handtekening over specifieke HTTP headers en de HTTP body te kunnen zetten om deze te beveiligen.

| `"sigD"` **header parameter** | **Beschrijving** | |
|---|---|---|
| `"mId"` | Als beschreven in ETSI TS 119 182-1, is een URI die het mechanisme voor refereren en verwerken van alle gerefereerde dataobjecten beschrijf, MOET gelijk zijn aan `"http://uri.etsi.org/19182/HttpHeaders"` | |
| `"pars"` | Als beschreven in ETSI TS 119 182-1, bevat een array van strings als parameters die met dit mechanisme getekend worden | |
| | **HTTP Header fields** | **Beschrijving** |
| | `"(request-target)"` | Enkel van toepassing voor HTTP requests |
| | `"host"` | Indien aanwezig |
| | `"content-type"` | Indien aanwezig |
| | `"content-encoding"` | Indien aanwezig |
| | `"digest"` | Indien aanwezig, het tekenen hiervan borgt dat de inhoud van de datadienst wordt gebonden aan de executie van de datadienst. |
| | `"LicensePurpose"` | Indien aanwezig, het tekenen hiervan kan borgen dat de licentie waaronder de data wordt gegeven wordt vastgelegd. |

Een JWT header ziet er bijvoorbeeld uit zoals hieronder:

Voorbeeld Geavanceerde JWT header

```
{
  "alg": "RS256",
  "b64": false,
  "crit":[
    "sigT",
    "sigD",
```

```
    "b64"
  ],
  "sigT":"2020-10-26T11:26:57Z",
  "sigD":{
    "pars":[
      "(request-target)",
      "host",
      "content-type",
      "content-encoding",
      "digest"
    ],
    "mId":"http://uri.etsi.org/19182/HttpHeaders"
  },
  "typ": "JOSE",
  "x5c":[
    "MIIGCDCCA/CgAwIBAgICEAQwDQYJKoZIhvcNAQELBQAwgZAxCzAJBgNVBAYTAk5MMQswCQYDVQQIDAJOSDEPMA0GA1UECgwGaVNIQVJ
    "MIIGBDCCA+ygAwIBAgICEAAwDQYJKoZIhvcNAQELBQAwgZAxCzAJBgNVBAYTAk5MMQswCQYDVQQIDAJOSDESMBAGA1UEBwwJQW1zdGV
    "MIIGCDCCA/CgAwIBAgIJAN7kMSjuGT9KMA0GCSqGSIb3DQEBCwUAMIGQMQswCQYDVQQGEwJOTDELMAkGA1UECAwCTkgxEjAQBgNVBAc
  ]
}
```


# JWT Payload

## Basis JWT

Het afsprakenstelsel volgt RFC7523 in het gebruik van de JWT payload.

✔️ Partijen MOETEN in alle Basis JWTs de JWT claims opstellen volgens het “JWT Bearer profile” als beschreven in RFC 7523 zoals opgesteld in de onderstaande tabel

| Claims | | Beschrijving |
|---|---|---|
| `iss` | VEREIST | Dit MOET een EORI nummer zijn als identificerend kenmerk, zoals gedefinieerd in Identificatie van Organisaties |
| `sub` | VEREIST | Dit MOET een EORI nummer zijn als identificerend kenmerk, zoals gedefinieerd in Identificatie van Organisaties |
| `aud` | VEREIST | Dit MOET een EORI nummer zijn als identificerend kenmerk, zoals gedefinieerd in Identificatie van Organisaties |
| `exp` | VEREIST | Als beschreven in RFC7523 |
| `iat` | VEREIST | Als beschreven in RFC7523 |
| `jti` | VEREIST | Als beschreven in RFC7523 |

Voor de borging van interoperabiliteit in het DSGO, is het een best practice om geen additionele datadienst specifieke JWT claims toe te voegen. Datadienst specifieke claims zouden in de resource moeten worden meegenomen

✔️ Partijen ZOUDEN in alle Basis JWTs NIET andere JWT claims MOETEN definiëren en gebruiken, afhankelijk van het specifieke gebruik van de JWT

✔️

Partijen MOETEN in alle Basis JWTs alle JWT claims binnen 30 seconden laten verlopen, aantoonbaar door de combinatie van `iat` en `exp` claims.

✔️ Partijen MOETEN in alle Basis JWTs de JWT claims de `iat` en `exp` claims noteren in seconden en MOGEN `iat` en `exp` claims NIET noteren in milliseconden

Een JWT payload voor een Basis JWT ziet er bijvoorbeeld uit zoals hieronder (Bron: iSHARE - JSON Web Token)

Voorbeeld Basis JWT payload

```
{
  "iss": "EU.EORI.NL123456789",
  "sub": "EU.EORI.NL123456789",
  "aud": "EU.EORI.NL987654321",
  "jti": "378a47c4-2822-4ca5-a49a-7e5a1cc7ea59",
  "exp": 1504683475,
  "iat": 1504683445
}
```

## Geavanceerde JWT

Het afsprakenstelsel volgt RFC7523 in het gebruik van de JWT payload.

✔️ Partijen MOETEN in alle Geavanceerde JWTs de JWT payload “detached“ maken van de handtekening, zoals beschreven in RFC 7515 Appendix F

✔️ Partijen MOETEN in alle Geavanceerde JWTs de JWT claims opstellen volgens de parameters zoals beschreven in `"sigD"` van de JWT Header.

Voor de borging van interoperabiliteit in het DSGO, is het een best practice om geen additionele datadienst specifieke JWT claims toe te voegen. Datadienst specifieke claims zouden in de resource moeten worden meegenomen

✔️ Partijen ZOUDEN in alle Geavanceerde JWTs NIET andere JWT claims MOETEN definiëren en gebruiken, afhankelijk van het specifieke gebruik van de JWT

Een JWT payload voor een Geavanceerde JWT ziet er bijvoorbeeld uit zoals hieronder TODO

Voorbeeld JWT payload

```
{
TODO
}
```

# JWT Verwerking

✔️ Partijen MOETEN een getekende JWT maar één keer accepteren

✔️ Partijen MOETEN een JWT niet accepteren als:

- De handtekening ongeldig is,

- Deze niet aan hen geadresseerd is, op basis van de `aud` claim,
- Deze niet verlopen is, op basis van de `exp` claim,
- Deze niet eerder ontvangen is, op basis van de `jti` claim met inachtneming van de verlooptijd,
- De geclaimde ondertekeningstijd, op basis van de `sigT` claim, niet valt binnen redelijke verwachte tijdvenster voor transacties vergeleken met de lokaal beheerde tijd

## JSON Web Encryptie (JWE)

JSON Web Encryptie (JWE) is een encryptie methode die toegepast kan worden om alle JWTs te beveiligen wanneer gesigneerde JWTs niet veilig genoeg zijn, beschreven in RFC 7516. Bijvoorbeeld wanneer informatie in JWT's niet onversleuteld gelogd mag worden. Wanneer dit gewenst is gegeven de specifieke context van een datadienst, kan dit worden toegepast. iSHARE geeft een beschrijving van het gebruik van JWE.

✔️ Partijen MOGEN gebruik maken van JWE als beschreven in RFC 7516

**Merk op,** Momenteel worden er geen afspraken gemaakt over JWE. Wanneer er meerdere security levels worden gedefinieerd of aanvullende beveiliging nodig is ten behoeve van use cases worden gedetailleerde afspraken over JWE mogelijk opgenomen in het afsprakenstelsel.

# Ondertekening

Het afsprakenstelsel maakt gebruik van QSEALS (Qualified Seal Certificates) voor het tekenen van JWTs om de integriteit en onweerlegbaarheid van interacties tussen partijen waar te borgen. Het tekenen van JWT die worden meegestuurd met alle API requests en responsen is een beveiligingsmechanisme die wordt toegepast boven op het beveiligen van het communicatieprotocol met TLS. QSEALS worden in lijn met de eIDAS regulering uitgegeven door gekwalificeerde vertrouwensdienstverleners op de List of Trusted Lists (LOTL).

✔️ Partijen MOETEN alle QSEALS gebruiken voor het tekenen van JWTs

✔️ Partijen MOETEN alle root certificaten voor QSEALs van CAs op de EU/EEA List of Trusted Lists (LOTL) en PKIO accepteren

# Onweerlegbaarheid

Voor sommige situaties is het van belang om waar te borgen dat ontvangst een bericht niet kan worden ontkend door de ontvangende of versturende partij. Dit geeft tevens de mogelijkheid om met terugwerkende kracht te kunnen valideren welke transacties, door wie en wanneer zijn uitgevoerd. Omdat onweerlegbaarheid niet in elke situatie noodzakelijk is, onweerlegbaarheid optioneel in het DSGO.

✔️ Als partijen willen dat een verzoek of respons onweerlegbaar is, MOETEN ze de `"Digest"` HTTP Header toevoegen in berichten zoals beschreven in de tabel hieronder.

✔️ Als partijen willen dat een bericht onweerlegbaar is, MOETEN ze een Geavanceerde JWT toevoegen in het bericht

| HTTP header | | Beschrijving |
|---|---|---|
| `Digest` | Optioneel | MOET volgens RFC 3230 worden gevuld met een SHA256 hash van de HTTP body, met bijpassende algorithme identifier S256 zoals gedefinieerd in ETSI TS 119 182-1 |

In het definiëren van datadiensten kunnen datadienstaanbieders ervoor kiezen dat onweerlegbaarheid in de datadienstrespons of datadienstverzoek van toepassing is.

✔️ Als datadienstaanbieders willen dat elke datadienstverzoek onweerlegbaar is, MOETEN ze dit vastleggen in de datadienstdefinitie

✔️ Als datadienstaanbieders onweerlegbare datadienstresponsen aanbied, MOETEN ze dit vastleggen in de datadienstdefinitie

# Juridische context

De juridische context van het afsprakenstelsel bestaat uit een overzicht van relevante wetgeving en actuele ontwikkelingen op nationaal en Europees niveau, waar het afsprakenstelsel ondergeschikt aan is, of op termijn mogelijk ondergeschikt aan wordt. In de volgende pagina's wordt de meest relevante juridische context voor afspraken, of het proces om te komen tot afspraken, in het afsprakenstelsel begrijpelijk gemaakt.

Deelnemende partijen zijn verantwoordelijk conform naar alle bestaande wet- en regelgeving te handelen. De gepresenteerde context is hier geen uitputtende lijst voor. De volgende wetgeving wordt beschreven:

> **Merk op**, de lijst van relevante wetgeving zal in volgende versies van het afsprakenstelsel mogelijk worden uitgebreid indien relevant.

- Mededingingsrecht
- Algemene Verordening Gegevensbescherming (AVG)
- Electronic Identification and Trust Services (eIDAS)
- Europa's data strategie (overkoepelend Europees beleid)
  - Data governance verordening (DGV)
  - Data verordening (DV)
- Domein specifieke wet-en regelgeving

# Mededingingsrecht

Gebruikers van het afsprakenstelsel moeten zich houden aan zowel het Nederlands als het Europees mededingingsrecht, zoals opgenomen in het Verdrag betreffende de werking van de Europese Unie. Voor het afsprakenstelsel zijn de onderwerpen betreffende kartelvorming en het misbruiken van economische machtsposities van het mededingingsrecht relevant.

- **Kartelverbod:** heeft betrekking op overeenkomsten of onderling afgestemde feitelijke gedragingen die mededinging op de Nederlandse en Europese markt beïnvloeden, hieronder valt onder andere coördinatie over het zetten van prijzen of contractuele voorwaarden. Afspraken binnen het afsprakenstelsel mogen er niet toe leiden dat mededinging op deze markten voor niet-deelnemende partijen beïnvloed wordt. Bovendien moet de toetredingsprocedure tot het afsprakenstelsel gelijk zijn voor iedere welwillende partij.
- **Economische machtspositie:** Het mededingingsrecht bepaalt dat ondernemingen hun economische machtspositie niet mogen misbruiken. Ondernemingen met een economische machtspositie moeten waarborgen dat concurrenten, leveranciers, afnemers en eindgebruikers, kunnen mededingen op de Nederlandse en Europese markt of een deel daarvan. Bij totstandkoming van en gedurende de continue ontwikkeling van het afsprakenstelsel, mogen partijen als gevolg van deze wetgeving geen afspraken afdwingen op basis van hun economische machtspositie.

# Algemene Verordening Gegevensbescherming (AVG)

De Algemene Verordening Gegevensbescherming (AVG) (in Engels: GDPR) is de Europese wetgeving die de data-privacy rechten van consumenten door de gehele EU waarborgt. De AVG is in mei 2018 in werking getreden. De AVG is van toepassing wanneer persoonsgegevens worden gedeeld of verwerkt.

## Persoonsgegevens

De AVG is uitsluitend van toepassing op persoonsgegevens.

:Quotes:

**Bron:** Europese Commissie - Wat zijn persoonsgegevens?

Persoonsgegevens zijn alle gegevens die betrekking hebben op een geïdentificeerde of identificeerbare levende natuurlijke persoon. Losse gegevens die samengevoegd kunnen leiden tot de identificatie van een bepaalde persoon vormen ook persoonsgegevens.

Persoonsgegevens waarbij de identiteitsgegevens zijn verwijderd, die zijn versleuteld of gepseudonimiseerd, maar die kunnen worden gebruikt om iemand opnieuw te identificeren, blijven persoonsgegevens en vallen binnen het toepassingsgebied van de AVG.

Persoonsgegevens die zo zijn geanonimiseerd dat de natuurlijke persoon niet of niet langer kan worden geïdentificeerd, worden niet langer als persoonsgegevens beschouwd. Gegevens zijn pas echt geanonimiseerd als de anonimisering onomkeerbaar is.

Voorbeelden van persoonsgegevens zijn onder andere, naam, adres, inkomen, cultureel profiel en een IP-adres. Vanuit de AVG zijn voorwaarden gesteld aan de data verwerker om persoonsgegevens te verwerken en daarmee indirect aan de betreffende persoon.

## Overzicht AVG

De AVG gaat over het rechtmatig omgaan met persoonsgegevens. De Autoriteit Persoonsgegevens geeft een duidelijk overzicht van de belangrijkste elementen van de AVG

:Quotes:

**Bron:** Autoriteit Persoonsgegevens - Belangrijkste bepalingen AVG

Persoonsgegevens mogen alleen worden verwerkt in overeenstemming met de wet. Voor de betrokkene (dat is degene van wie de persoonsgegevens verwerkt worden) moet het behoorlijk en transparant zijn hoe en waarom de persoonsgegevens verwerkt worden.

Persoonsgegevens mogen alleen verzameld worden met een gerechtvaardigd doel. Dat doel moet welbepaald zijn en vooraf uitdrukkelijk zijn omschreven. Het doel waarvoor een organisatie de persoonsgegevens gaat verwerken moet verenigbaar zijn met het doel waarmee de persoonsgegevens zijn verzameld.

Verwerkt een organisatie of persoon persoonsgegevens? Dan moet de persoon van wie de persoonsgegevens worden verwerkt in ieder geval op de hoogte zijn van de identiteit van de organisatie of persoon die deze persoonsgegevens verwerkt (de zogeheten verwerkingsverantwoordelijke) en van het doel van de gegevensverwerking.

Als organisaties persoonsgegevens verwerken, dan moeten ze daarbij als uitgangspunt hanteren ‘zo min mogelijk’. Dat houdt o.a. in dat de verwerking van de gegevens moet passen bij het doel waarvoor ze worden verwerkt.

De verwerkingsverantwoordelijke moet ervoor zorgen dat de gegevens juist zijn en zo nodig worden geactualiseerd.

De gegevensverwerking moet op een passende manier worden beveiligd. Voor bijzondere gegevens, zoals over ras, gezondheid en geloofsovertuiging, gelden extra strenge regels.

## Grondslagen voor het verwerken van persoonsgegevens

Volgens de AVG moeten partijen een grondslag hebben om persoonsgegevens te verwerken, in de AVG zijn zes grondslagen opgesteld.

:Quotes:

**Bron:** Autoriteit Persoonsgegevens - Mag ik uw persoonsgegevens verwerken?

In de AVG staan de volgende 6 grondslagen voor het verwerken van persoonsgegevens:

1. U heeft toestemming van de persoon om wie het gaat.
2. Het is noodzakelijk om gegevens te verwerken om een overeenkomst uit te voeren.
3. Het is noodzakelijk om gegevens te verwerken omdat u dit wettelijk verplicht bent.
4. Het is noodzakelijk om gegevens te verwerken om vitale belangen te beschermen.
5. Het is noodzakelijk om gegevens te verwerken om een taak van algemeen belang of openbaar gezag uit te oefenen.
6. Het is noodzakelijk om gegevens te verwerken om uw gerechtvaardigde belang te behartigen.

## Relevantie voor het afsprakenstelsel

Het afsprakenstelsel is data agnostisch, en beschrijft niet welke data uitgewisseld wordt. Het is mogelijk dat er middels datadiensten persoonsgegevens worden uitgewisseld. Bijvoorbeeld data gerelateerd aan medewerkers of klanten van deelnemende partijen. Wanneer dit het geval is moeten datadienstaanbieders en datadienstgebruikers aan de AVG voldoen om de persoonsgegevens te beschermen.

# Electronic Identification and Trust Services (eIDAS)

De Europese verordening voor elektronische identificatie en vertrouwensdiensten regelt de randvoorwaarden voor elektronische transacties in de interne markt. Ze wordt meestal aangeduid als eIDAS en de Engelse benaming Electronic Identification and Trust Services.

eIDAS bestaat uit twee belangrijke delen:

1. **elektronische identificatie**: In hoofdstuk II wordt geregeld dat mensen en organisaties authenticatiemiddelen uit nationale elektronische identiteit (eID), zoals eHerkenning of DigiD, kunnen gebruiken bij publieke diensten in alle EU lidstaten.
2. **vertrouwensdiensten**: In hoofdstuk III wordt een Europese interne markt voor vertrouwensdiensten (zoals elektronische handtekeningen, zegels, archivering en certificaten voor websiteauthenticatie) geregeld, door te borgen dat deze EU lidstaat overstijgend werken en dezelfde juridische werking hebben als de papiergebaseerde equivalenten.

## Relevantie voor het afsprakenstelsel

Voor de private datadiensten binnen het afsprakenstelsel heeft hoofdstuk II van eIDAS geen dwingende werking. Echter, net als in afsrpakenstelsels als eHerkenning en iSHARE, ligt het wel voor de hand om de concepten uit dat deel (zoals betrouwbaarheidsniveaus) in het afsprakenstelsel te hergebruiken binnen het onderwerp van authenticatie.

Hoofdstuk III van eIDAS is direct bruikbaar voor het afsprakenstelsel. De vertrouwensdiensten voor authenticatie van websites en elektronische zegels worden, net als in iSHARE, gebruikt voor de authenticatie van organisaties op verbinding niveau en respectievelijk het verzegelen van berichten die worden uitgewisseld tussen organisaties.

Waar gebruik wordt gemaakt van eIDAS wordt expliciet verwezen naar het specifieke relevante deel van de verordening.

> N.B. komt er met de herziening van eIDAS, naar verwachting in 2025 een EU Digital Identity Wallet beschikbaar. Burgers en werknemers kunnen zich hiermee identificeren en credentials delen. Momenteel lopen hiervoor op grote schaal pilots. Het DSGO volgt de ontwikkelingen nauwgezet.

# Europa's data strategie (overkoepelend Europees beleid)

In februari 2020 heeft de Europese Commissie de Europese data strategie aangekondigd. De data strategie moet zorgen voor een interne Europese markt voor data, en een eerlijke, veilige en dynamische Europese data economie. Als onderdeel hiervan zijn twee concept-verordeningen opgesteld waarvan de Data governance verordening (DGV) al goedgekeurd is:

- Data governance verordening (DGV)
- Data verordening (DV)

# Data governance verordening (DGV)

De Data governance verordening (DGV) stimuleert om meer data beschikbaar te stellen door instanties de mogelijkheden (technieken, tools en eisen voor tussenpartijen) hiervoor te geven. De DGV is op 23 juni 2022 in werking getreden en wordt na een overgangsperiode van 15 maanden in september 2023 verplicht gesteld. O.a. de volgende mechanismes staan beschreven in de DGV:

- **Hergebruik van beschermde gegevens bij overheidsinstanties:** Overheidsinstanties kunnen beschermde gegevens beschikbaar stellen door gebruik te maken van beschreven mechanismen (bijvoorbeeld het ter beschikking stellen van een veilige verwerkingsomgeving of gegevens aggregeren) en hiermee voldoen aan privacy vereisten en vertrouwelijkheidsverplichtingen.
- **Rollen om data delen makkelijk en vertrouwd te maken**
  - *Databemiddelingsdiensten*: een derde partij die gegevenshouders verbinden aan gegevensgebruikers, deze gegevens niet gebruikt voor andere doeleinden dan beschikbaarstelling aan gegevensgebruikers en dit doet via een afzonderlijke rechtspersoon. Databemiddelingsdiensten moeten zich hierbij aan een strikte set regels houden.
  - *Data altruïsme organisaties*: organisaties die, met toestemming van datasubjecten, gegevens beschikbaar willen stellen, zonder tegenprestatie. Organisaties kunnen zich vrijwillig laten erkennen als ‘erkende organisaties voor data altruïsme’.
- **Europees Comité voor gegevensinnovatie:** Comité dat richtsnoeren voorstelt om sectorspecifieke of sectoroverschrijdende interoperabiliteit te realiseren.

## Relevantie voor het afsprakenstelsel

De DGV legt verplichtingen op aan databemiddelingsdiensten, erkende organisaties voor data altruïsme of organisaties die gebruik maken van de mechanismen als gedefinieerd in de DGV. De DGV is hiermee niet voor iedere deelnemer van het afsprakenstelsel van toepassing. Voor partijen die als databemiddelaar of data altruïsme organisatie deelnemen aan het afsprakenstelsel gelden mogelijk afwijkende afspraken dan voor andere deelnemers. Bijvoorbeeld over de compensatie voor datadiensten ten opzichte van individuele partijen, over de totale compensatie in verhouding tot de gemaakte kosten voor het aanbieden van datadiensten.

# Data verordening (DV)

De Data verordening (DV) beschrijft geharmoniseerde regels voor eerlijke toegang tot en eerlijk gebruik van data om een eerlijker speelheld te creëeren voor data-aanbieders en -gebruikers. De DV is op 23 februari 2022 voorgesteld door de Europese Commissie en wordt momenteel herzien door de Europese Raad. De DV is daarmee nog aan verandering onderhevig.

De DV gaat o.a. in op de volgende onderwerpen:

- **Gebruikers krijgen het recht op toegang tot en gebruik van data (voor derden):** Ondernemingen die producten of gerelateerde diensten aanbieden die bij gebruik data genereren, bijvoorbeeld IoT producten en sensoren, worden verplicht om deze data, op aanvraag, beschikbaar te stellen voor de gebruikers of derde partijen (inclusief mogelijk concurrenten van deze aanbieders). Voor ontvangende derde partijen gelden specifieke verplichtingen, deze zijn aangegeven in artikel 6.
- **Data beschikbaar stellen voor overheidsinstanties:** Ondernemingen worden verplicht om data, onverwijld, beschikbaar te stellen aan publieke instellingen in het geval van een uitzonderlijke noodzaak, bijvoorbeeld bij een natuurlijke of medische ramp.
- **Oneerlijke bedingen:** Kleine-, micro- en middelgrote ondernemingen moeten eerlijk, niet discriminerend, transparant en op een redelijke wijze behandeld worden bij contractuele bedingen betreft de toegang tot en het gebruik van data.

## Relevantie voor het afsprakenstelsel

De DV is relevant bij het bepalen van rechthebbende partijen en autorisaties.

De DV bepaalt dat meerdere partijen, (mogelijk verschillende) rechten hebben over data voortkomend uit data-generende producten of gerelateerde diensten (bijvoorbeeld sensoren). Hiermee kunnen de rechthebbende partijen verschillen afhankelijk van de doeleinden van datadiensten. Het is de verantwoordelijkheid van datadienstaanbieders om te weten wie de rechthebbende partijen zijn over data in door hen aangeboden datadiensten.

Bovendien bepaalt de DV dat in het geval van uitzonderlijke noodzaak, publieke partijen die door de rechthebbende normaliter niet geautoriseerd zijn tot datadiensten zonder inspraak van de rechthebbende wel geautoriseerd worden.

# Domein specifieke wet-en regelgeving

Hier zal een overzicht volgen over wet- en regelgeving specifiek voor de gebouwde omgeving.

Wat hier mogelijk in terugkomt:

- Bepalingen aangaande bestekken en consortia
- De relatie tussen het DSGO en het Digitaal Stelsel Omgevingswet (DSO)
- Hoe het DSGO zich verhoudt tot de wettelijke basisregistraties

# Service level agreements

SLAs (Service Level Agreements) zijn afspraken over de kwaliteit, beschikbaarheid en verantwoordelijkheden van de datadienstaanbieder bij een te leveren datadienst. Een minimale set van eisen over SLAs zorgt ervoor dat voor alle betrokken partijen duidelijk is wat ze kunnen verwachten van aangeboden datadiensten in het DSGO. Voor datadienstgebruikers is een dit essentieel om business processen te laten baseren op datadiensten. Hieronder worden twee bestaande voorbeelden van SLAs uit de gebouwde omgeving gegeven.

⭐ **Voorbeelden**: Binnen de gebouwde omgeving bestaan een groot aantal digitale diensten beschikbaar, met bijhorende SLAs. Ter illustratie worden er twee verschillende voorbeelden gepresenteerd.

- Publieke Dienstverlening Op de Kaart (PDOK) is een platform voor het ontsluiten van geodatasets van Nederlandse overheden. De servicelevels van PDOK zijn hier beschikbaar.
- Cadac Group zijn (o.a.) resellers van Autodesk software. De servicelevels voor de diensten van Cadac zijn hier beschikbaar.

Voor de verschillende rollen geïdentificeerd binnen het afsprakenstelsel zijn de SLAs vast gelegd:

- SLAs voor Datadienstaanbieders
- SLAs voor de Beheerorganisatie

De SLAs in het afsprakenstelsel zijn in lijn met die van iSHARE en dragen daarmee bij aan interoperabiliteit tussen DSGO en iSHARE.

# SLAs voor Datadienstaanbieders

Voor datadienstaanbieders in het afsprakenstelsel gelden de SLAs vermeld op deze pagina. SLAs van datadiensten zijn een onderdeel van de datadienstdefinitie.

## Beschikbaarheid

Beschikbaarheid geeft aan wat de eisen zijn over de tijd dat een datadienst werkend is. Beschikbaarheid wordt gedefinieerd door de volgende vensters:

- **Openstellingsvenster –** De periode dat de datadienst beschikbaar wordt gesteld en door datadienstgebruikers te benaderen is.
- **Onderhoudsvenster –** De tijden dat regulier onderhoud van de datadienst plaatsvindt. Tijdens het onderhoudsvenster kan het voorkomen dat (onderdelen van) de datadienst niet beschikbaar zijn.
- **Beschikbaarheidsvenster –** De tijden binnen het openstellingsvenster waarbij de datadienstaanbieder garanties voor de datadienst afgeeft. Gelijk aan het openstellingsvenster min het onderhoudsvenster.

Om flexibiliteit te bieden aan het ontwerpen van datadiensten, worden er geen eisen gesteld aan datadienstaanbieders voor de specifieke openstellingsvenster van de datadiensten die ze definiëren. Merk op, het oplossen van incidenten maakt geen deel uit van regulier onderhoud, en valt niet onder de beschikbaarheidsvenster zoals beschreven (zie Incidentenbeheer voor meer informatie).

✔️ Datadienstaanbieders MOETEN het openstellingsvenster van de datadienst definiëren en beschikbaar stellen aan datadienstgebruikers

✔️ Datadienstaanbieders MOETEN het onderhoudsvenster van de datadienst definiëren en beschikbaar stellen aan datadienstgebruikers

✔️ Datadienstaanbieders MOETEN het onderhoudsvenster plannen buiten reguliere kantooruren

✔️ Datadienstaanbieders MOGEN gepland onderhoud uitvoeren op elke tijdstip, als er geen uitval wordt verwacht

✔️ Datadienstaanbieders ZOUDEN datadiensten binnen het beschikbaarheidsvenster minimaal 95% van de tijd beschikbaar MOETEN stellen aan datadienstgebruikers

ℹ️ **Merk op**, hoe datadienstaanbieders kunnen voldoen aan de bovenstaande eisen zal verder worden gedetailleerd als operationeel proces. Deze wordt op een later moment uitgewerkt

## Prestatie

Prestatie geeft de tijd aan waarin een partij moet reageren op een API verzoek en wordt gemeten in tijd of aantallen. De prestatie van een datadienst is nodig voor de waarborging van de kwaliteitsbeleving van datadienstgebruikers.

✔️ Datadienstaanbieders ZOUDEN op 95% van API verzoeken binnen 2 seconden MOETEN reageren binnen het beschikbaarheidsvenster

✔️ Datadienstaanbieders ZOUDEN op 99% van API verzoeken binnen 5 seconden MOETEN reageren binnen het beschikbaarheidsvenster

✔️ Datadienstaanbieders ZOUDEN ten minste 100 API verzoeken MOETEN kunnen verwerken binnen het beschikbaarheidsvenster

## Continuïteit

In het geval van een incident, is het van belang dat een datadienst na afhandeling van een incident efficiënt kan worden hersteld en beschikbaar kan worden gesteld. Om dit doel te bereiken zijn er SLAs opgesteld rondom de opslag van data (back-up).

✔️ Datadienstaanbieders ZOUDEN op een passende frequentie een back-up MOETEN maken van data belangrijk voor de datadienst

✔️ Datadienstaanbieders ZOUDEN de back-ups MOETEN opslaan voor een passende periode

## Ondersteuning

Ondersteuning betreft de hulp of assistentie bij vragen, verzoeken en klachten van partijen of het beheer. Het is aan de datadienstaanbieder om geschikte ondersteuning te bieden, de volgende eisen gelden als minimale best practices voor het bieden van ondersteuning van datadiensten.

✔️ Datadienstaanbieders ZOUDEN bereikbaar MOETEN zijn voor ondersteuning via e-mail

✔️ Datadienstaanbieders ZOUDEN binnen een werkdag na ontvangst van een vraag, verzoek of klacht MOETEN aangeven dat hiervan kennis is genomen

✔️ Datadienstaanbieders ZOUDEN binnen vijf werkdagen na ontvangst van een vraag, verzoek of klacht deze MOETEN beantwoorden of oplossen

## Releasebeheer

Releasebeheer bevat o.a. het proces van het testen, uitrollen en controleren van datadiensten. Binnen het afsprakenstelsel zijn er eisen gelegd aan het uitbrengen van updates op datadiensten om de integriteit van het ecosysteem te behouden.

✔️ Datadienstaanbieders MOETEN aan alle releasebeheer eisen voldoen

ℹ️ Merk op, de gedetailleerde releasebeheer-eisen zullen door de (toekomstige beheerorganisatie) worden gedetailleerd als operationeel proces. Deze wordt op een later moment uitgewerkt

# SLAs voor de Beheerorganisatie

Momenteel wordt de toekomstige beheerorganisatie van het afsprakenstelsel opgezet. Wanneer er meer duidelijkheid is over de verantwoordelijkheden van de beheerorganisatie worden SLAs voor het beheer opgesteld.

# Operationele processen

Deze sectie beschrijft de operationele processen die nodig zijn voor deelnemers om deel te kunnen nemen en om het ecosysteem operationeel te draaien. Op termijn zullen deze processen operationeel zijn onder Beheer.

- Toetreding tot het DSGO
- Toezicht en handhaving
- Change en release management

# Toetreding tot het DSGO

Partijen die willen toetreden in de rol van datadienstaanbieder, authenticatiedienst en/of autorisatieregister moeten het toetredingsproces doorlopen. Het toetredingsproces beschrijft de stappen die een potentiële deelnemer moet nemen om toe te treden tot het DSGO. Het DSGO kent één generiek toetredingsproces met daarin variaties die het proces specifiek maken voor de verschillende rollen. Na het succesvol doorlopen van de toetredingsproces mag een partij acteren volgens de rechten en plichten van de rol als welke een partij is toegetreden.

## Doelstelling

Het toetredingsproces bestaat zodat een potentiële deelnemer kan aantonen dat zij in staat is om conform de afspraken voor de rol waarin zij wil toetreden te kunnen functioneren.

## Verantwoordelijkheden

Bij het doorlopen van het toetredingsproces heeft zowel de DSGO beheerorganisatie als de potentiële deelnemer verantwoordelijkheden

### Beheerorganisatie

De beheerorganisatie is verantwoordelijk dat iedere deelnemer het toetredingsproces juist heeft doorlopen en wordt geacht de potentiële deelnemers hierin te ondersteunen mocht dit nodig zijn

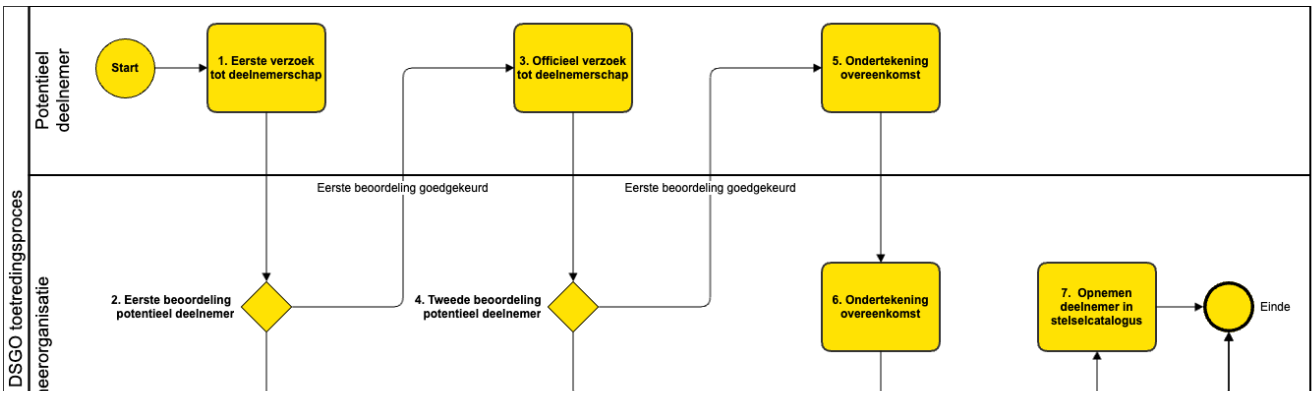
- De beheerorganisatie MOET een potentiële deelnemer door het toetredingsproces begeleiden
- De beheerorganisatie MOET zorgen dat een potentiële deelnemer toegang heeft tot de DSGO conformiteitstesttool
- De beheerorganisatie MOET een non disclosure agreement (NDA) tekenen tijdens het testen mocht de potentiële deelnemer daarom vragen

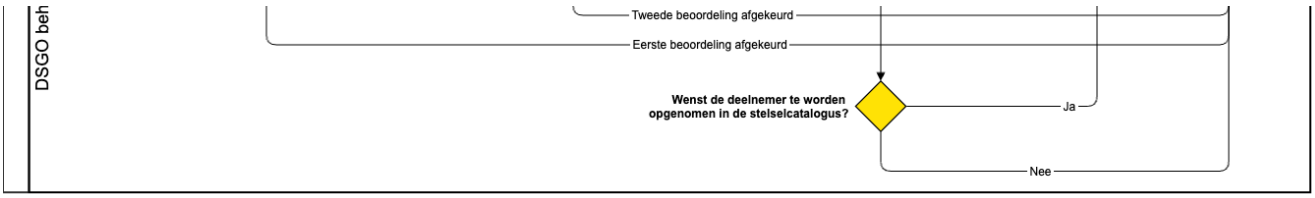
### Potentiële deelnemer

Een potentiële deelnemers is verantwoordelijk om aan de beheerorganisatie aan te tonen dat ze aan alle vereisten voor toetreding voldoen

- Partijen MOETEN de benodigde informatie en/of documenten voor toetreding op de manier aanleveren die door de DSGO beheerorganisatie vereist wordt

## Proces






1. Een potentiële deelnemer maakt bij de DSGO beheerorganisatie kenbaar deelnemer te willen worden. Hierbij stuurt de potentiële deelnemer de onderstaande informatie op naar de DSGO beheerorganisatie:
   a. Administratieve informatie zijnde bedrijfsnaam zoals bij bekend bij de kamer van koophandel, contactinformatie (e-mailadres & telefoonnummer) op organisatieniveau, contactinformatie van een (e-mailadres & telefoonnummer) bereikbare werknemer gedurende het toetredingsproces
   b. Een duiding als welke rol de potentiële deelnemer wil toetreden tot het DSGO
   c. Een valide EORI-nummer zoals bekend bij de Kamer van Koophandel
2. De DSGO beheerorganisatie controleert de aangeleverde informatie en beoordeeld of er geen indicaties zijn dat het vertrouwen in en functioneren van het DSGO nadelig beïnvloedt wordt bij toetreding van de potentiële deelnemer, indicaties hiervan zijn bijvoorbeeld (niet-uitputtend):
   a. Eerder uitgesloten zijn van het DSGO of andere samenwerkingsinitiatieven
   b. Lopende rechtszaken jegens de potentiële deelnemer
3. De potentiële deelnemer dient een officieel verzoek in om deelnemer te worden van het DSGO en toont aan te kunnen voldoen aan de vereisten passend bij de toekomstige rol
   a. **Een potentieel datadienstaanbieder:**
      i. Toont aan een (dummy) datadienst uit te kunnen voeren door deze succesvol te toetsten in de DSGO conformiteitstesttool zoals beschreven op de pagina …
      ii. Stelt een datadienstdefinitie op zoals beschreven op de pagina Trust Framework catalog - data service definition en toont met de DSGO conformiteitstesttool aan deze te kunnen registreren zoals op pagina … . *Let wel: Dit is alleen vereist mits de potentieel datadienstaanbieder bij toetreding direct een datadienst wil registreren*
   b. **Een potentiële authenticatiedienst:**
      i. Toont de gedefinieerde diensten voor authenticadiediensten uit te kunnen voeren door deze succesvol te testen in de DSGO conformiteitstesttool zoals beschreven op de pagina …
      ii. Toont via het iSHARE assessment framework aan operationele processen voor authenticatiediensten conform het afsprakenstelsel uit te kunnen voeren
   c. **Een potentieel autorisatieregister:**
      i. Toont aan de gedefinieerde diensten voor autorisatieregisters uit te kunnen voeren door deze succesvol te testen in de DSGO conformiteitstesttool zoals beschreven op de pagina …
      ii. Toont ia het iSHARE assessment framework aan operationele processen voor autorisatieregsters conform het afsprakenstelsel uit te kunnen voeren
4. De DSGO beheerorganisatie beoordeeld of de potentiële deelnemer mag toetreden tot het stelsel:
   a. De DSGO beheerorganisatie heeft in het geval de potentiële deelnemer wil toetreden als datadienstaanbieder 5 dagen om het verzoek te beoordelen en bij goedkeuring de deelname-overeenkomst op te sturen. Wanneer een verzoek niet goedgekeurd wordt moet de DSGO beheerorganisatie dit toelichten
   b. De DSGO beheerorganisatie heeft in het geval de potentiële deelnemer wil toetreden als authenticatiedienst of autorisatieregister 30 dagen om het verzoek te beoordelen en bij goedkeuring de deelname-overeenkomst op te sturen. Wanneer een verzoek niet goedgekeurd wordt moet de DSGO beheerorganisatie dit toelichten
5. De potentiële deelnemer ondertekend de deelname-overeenkomst en stuurt deze op naar de DSGO beheerorganisatie
6. Een wettelijke vertegenwoordiger van de DSGO beheerorganisatie ondertekend en treedt de potentiële deelnemer als datadienstaanbieder, authenticatiedienst en/of autorisatieregister toe tot het DSGO
7. De DSGO beheerorganisatie neemt de onderstaande informatie op in de stelselcatalogus en communiceert het toetreden van de deelnemer met de andere deelnemers, mits dit deelnemer hiermee akkoord gaat:
   a. Naam en identificerend kenmerk van de deelnemer

Wanneer een huidig deelnemer een extra of andere rol in het DSGO wil invullen, moet de deelnemer het toetredingsproces specifiek voor de desbetreffende rol opnieuw doorlopen.

# Toezicht en handhaving

Om data delen tussen partijen mogelijk te maken is onderling vertrouwen een van de voorwaarden. Voor het creëren van onderling vertrouwen tussen betrokken partijen is het essentieel dat de afspraken uit het afsprakenstelsel nageleefd worden. De beheerorganisatie DSGO houdt toezicht op de naleving van het afsprakenstelsel en kan ondersteunen bij het herstellen van incidenten die het onderling vertrouwen kunnen schaden. Als stok achter de deur kan de beheerorganisatie ook sancties opleggen bij overtredingen van de afspraken uit het stelsel.

## Toezicht

In het afsprakenstelsel is toezicht tweeledig en bestaat uit actief en passief toezicht.

### Actief toezicht

Actief toezicht vindt plaats gedurende het toetredingsproces van partijen, bij het registreren van datadiensten, en bij regelmatige audits van voorzieningen. Bij het toetredingsproces dienen potentiële deelnemers aan te tonen dat ze in staat zijn om conform het afsprakenstelsel te functioneren (zie Toetreding). Bij het registeren van datadiensten wordt actief toezicht gehouden. De datadienstaanbieder dient aan te tonen dat haar datadienst voldoet aan de relevante afspraken uit het afsprakenstelsel voordat de datadienst live gaat. Verder worden alle voorzieningen binnen het DSGO regelmatig ge-audit om te zorgen dat aan de afspraken wordt gehouden.

> **Merk op,** het afsprakenstelsel is nog in ontwikkeling. Het proces van datadienst registratie, en audits van voorzieningen worden in een volgende versie van het afsprakenstelsel verder uitgewerkt.

### Passief toezicht

De beheerorganisatie houdt passief toezicht op het functioneren van het DSGO. Alle partijen die betrokken zijn bij het DSGO kunnen een incident melden wanneer er een ongewenste gebeurtenis plaatsvindt. Wanneer een incident wordt gemeld wordt deze in een gestandaardiseerd proces behandeld (zie Incidentbeheer).

> **Merk op,** Naast intern toezicht dienen deelnemers ook rekening te houden met extern toezicht door bij wet aangestelde toezichthouders. Externe toezicht op de toepasselijke wetgeving wordt uitgevoerd door de daartoe bevoegde (overheids)instanties en valt buiten scope van het afsprakenstelsel (zie Juridische context).

## Handhaving

Indien er sprake is van een overtreding, kan de beheerorganisatie, parallel aan het incidentbeheer proces een handhavingsproces starten. De beheerorganisatie kan in dit proces 3 verschillende sancties opleggen: een waarschuwing, een schorsing en uitsluiting (zie Handhaving).

# Incidentbeheer

De beheerorganisatie DSGO houdt passief toezicht op het naleven van het afsprakenstelsel door te handelen bij melding van een incident. Wanneer de melding binnenkomt zal de beheerorganisatie een neutrale incidentcoördinator aanwijzen die het incidentbeheer proces zal leiden. Het incidentbeheer proces is het gehele proces van melding van een incident tot afronding van het incident. Een incident wordt in het DSGO gedefinieerd als:

Een ongewenste gebeurtenis die niet direct oplosbaar is en:

- Niet tot de standaardoperatie van het DSGO en/of de beschikbare datadiensten behoort, en/of
- Mogelijk leidt tot het verlies van vertrouwen, veiligheid en integriteit van het afsprakenstelsel en/of datadiensten geïmplementeerd op het afsprakenstelsel.

Een incident kan door iedere bij het DSGO betrokken partij gemeld worden wanneer zij constateert of het vermoeden heeft dat een partij zich niet aan het afsprakenstelsel houdt. In het afsprakenstelsel worden incidenten in drie classificaties onderverdeeld (zie classificatie incidenten).

## Doelstelling

Het toezicht van de beheerorganisatie op de naleving van het afsprakenstelsel door alle betrokken partijen heeft als doel de betrouwbaarheid van het DSGO te borgen. Naleving van het afsprakenstelsel is cruciaal voor de betrouwbaarheid en vertrouwen in het DSGO. De eerste vorm van toezicht gebeurt bij toetreding van deelnemers en bij de registratie van datadiensten. Hierna zal de beheerorganisatie passief toezicht houden op basis van ingekomen meldingen van incidenten.

## Verantwoordelijkheid

Alle partijen die gebruikmaken van het afsprakenstelsel hebben een verantwoordelijkheid in incidentbeheer.

### Beheerorganisatie

Het is de verantwoordelijkheid van de beheerorganisatie om bij ontvangst van een incident melding op te treden als toezichthouder. Daarnaast is de beheerorganisatie ook verantwoordelijk voor het aanstellen van een neutrale incidentcoördinator. Wanneer de beheerorganisatie zelf niet betrokken is bij een incident zal de beheerorganisatie als incidentcoördinator optreden.

✔️ De beheerorganisatie MOET een incidentcoördinator aanwijzen na een melding van een incident

### Betrokken partijen

Iedere bij het DSGO betrokken partij heeft de verantwoordelijkheid om bij de beheerorganisatie een incident te melden wanneer zij niet-naleving van het afsprakenstelsel constateert of vermoedt. Verder zijn bij een Prioriteit 1 of 2-incident betrokken partijen verantwoordelijk voor het beschikbaar stellen van een incidentmanager voor de afhandeling van het incident.

✔️ Partijen MOETEN incidenten direct na ontdekking melden bij de beheerorganisatie

✔️ Partijen ZOUDEN voor alle Prioriteit 1 en Prioriteit 2 incidenten waarbij zij betrokken zijn een incidentmanager 24u per dag, 7 dagen per week beschikbaar MOETEN stellen

✔️ Partijen MOETEN voor alle Prioriteit 1 en Prioriteit 2 incidenten waarbij zij betrokken zijn een incidentmanager beschikbaar stellen

### Incidentcoördinator

Voor elk incident wordt een (neutrale) incidentcoördinator aangewezen door de beheerorganisatie. De incidentcoördinator is verantwoordelijk voor het coördineren van het incidentbeheer proces. De incidentcoördinator moet altijd een neutrale partij zijn. Afhankelijk van de eventuele betrokkenheid van de beheerorganisatie bij een incident kan de rol van incidentcoördinator worden uitgevoerd door de beheerorganisatie of door een externe partij.

✔️ De incidentcoördinator MOET het incidentbeheer proces na de melding van een incident coördineren.

✔️ De incidentcoördinator MOET kunnen optreden als een neutrale partij bij het incident

### Incidentmanager

De incidentmanager is (een contactpersoon) van een bij het incident betrokken partij die verantwoordelijk is voor het verhelpen of oplossen van incidenten.

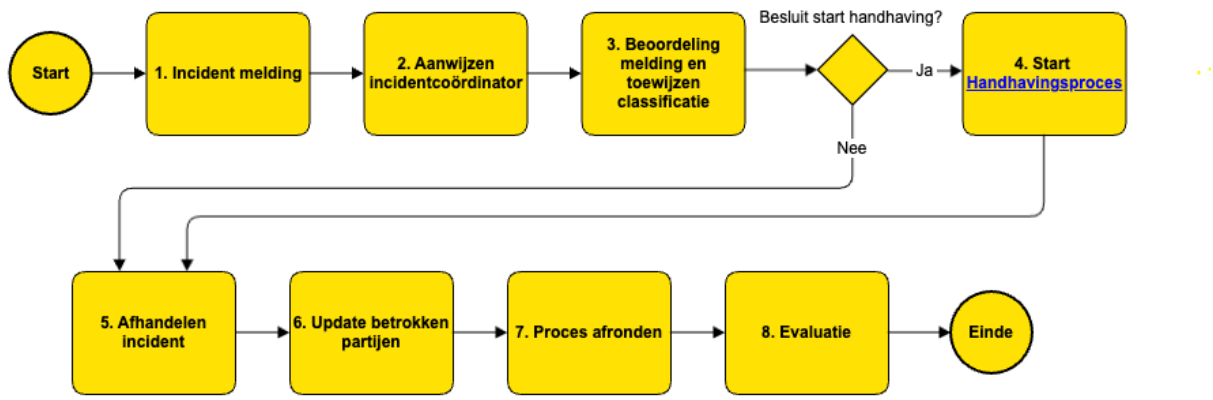
✔️ De incidentmanager MOET voor een Prioriteit 1 incident een update delen met de incidentcoördinator binnen 2 uur van elke belangrijke update en elke 4 uur bij geen update

✔️ De incidentmanager MOET voor een Prioriteit 2 incident een update delen met de incidentcoördinator binnen 2 uur van elke belangrijke update aan het einde van elke werkdag bij geen update

✔️ De incidentmanager MOET voor een Prioriteit 3 incident een volledige update delen met de incidentcoördinator aan het einde van elke werkdag

## Incidentbeheer Proces

Onderstaand figuur geeft een globaal beeld van de stappen in het incidentbeheer proces, deze wordt in detail beschreven onder het figuur.




Het incidentbeheer proces is als volgt:

1. **Incident melding:** Een bij het DSGO betrokken partij meldt bij de beheerorganisatie een incident dat zich heeft voorgedaan en levert daar de volgende informatie bij aan:
   - De naam van de verondersteld veroorzakende partij, onderbouwing van de constatering/vermoeden, datum, tijd, ingeschatte incident classificatie en impact op de datadienst.

2. **Aanwijzing incidentcoördinator:** De beheerorganisatie wijst een incidentcoördinator aan. Als de beheerorganisatie niet betrokken is bij het incident zal zij zelf die rol op haar nemen. Indien de beheerorganisatie betrokken is bij het incident wijst zij een neutrale externe partij aan die de rol van incidentcoördinator op zich neemt.
3. **Beoordeling melding en toewijzen classificatie:** De incidentcoördinator beoordeelt de melding en de inschatting van classificatie van het incident:
   a. Accepteert de classificatie en gaat door naar stap 4, of
   b. Verandert de classificatie en gaat door naar stap 4, of
   c. Verwerpt de melding en informeert hier de betrokken partijen over
4. **Besluit start handhavingsproces:** Op basis van de ingekomen melding kan de beheerorganisatie besluiten om een handhavingsproces te starten. (Zie handhaving)
5. **Afhandeling incident:** De incidentcoördinator registreert het incident en start een voorgeschreven procedure
   a. De procedure bij een melding geclassificeerd als een Prioriteit 3 melding:
      i. De incidentcoördinator geeft de meldende partij, de veroorzakende partij en/of (een) andere betrokken partij(en) - afhankelijk van wat zij het meest geschikt acht - de verantwoordelijkheid voor het afhandelen van het incident, onder supervisie van de incidentcoördinator (zie stap 5).
      ii. De partij(en) die verantwoordelijk is/zijn voor de afhandeling van het incident communiceert/communiceren het incident, de aangewezen incidentmanager en dat het incident wordt opgelost naar betrokken partijen.
   b. De procedure bij een melding geclassificeerd als een Prioriteit 2 melding:
      i. De incidentcoördinator geeft de meldende partij, de veroorzakende partij en/of (een) andere betrokken partij(en) - afhankelijk van wat zij het meest geschikt acht - de verantwoordelijkheid voor het afhandelen van het incident, onder supervisie van de incidentcoördinator (zie stap 5).
         1. Indien er sprake is van een inbreuk op de gegevensbeveiliging die gemeld moet worden volgens de meldplicht datalekken, meldt (melden) de verantwoordelijke(n) voor de afhandeling van het incident de inbreuk op de gegevensbeveiliging bij de Autoriteit Persoonsgegevens en volgt (volgen) de richtlijnen van de Autoriteit Persoonsgegevens voor de rest van het incidentbeheer proces.
      ii. De incidentcoördinator, in samenwerking met de beheerorganisatie, informeert alle partijen in het DSGO en relevante partijen daarbuiten (bijv. brancheorganisaties, het NCSC of zelfs wetshandhaving) over het incident (en dat deze wordt opgelost), wie de incidentmanager is en wie de incidentcoördinator is.
      iii. De incidentcoördinator stelt een actieplan op om risico's en schade te minimaliseren.
   c. De procedure bij een melding geclassificeerd als een Prioriteit 1 melding:
      i. De incidentcoördinator geeft de meldende partij, de veroorzakende partij en/of (een) andere betrokken partij(en) - afhankelijk van wat zij het meest geschikt acht - de verantwoordelijkheid voor het afhandelen van het incident, onder supervisie van de incidentcoördinator (zie stap 5). Anders dan bij Prioriteit 2 of 3 meldingen kan de incidentcoördinator er ook voor kiezen om zelf de verantwoordelijkheid voor de afhandeling van de Prioriteit 1 melding op zich te nemen.
         1. Indien er sprake is van een inbreuk op de gegevensbeveiliging die gemeld moet worden volgens de meldplicht datalekken, meldt (melden) de verantwoordelijke(n) voor de afhandeling van het incident de inbreuk op de gegevensbeveiliging bij de Autoriteit Persoonsgegevens en volgt (volgen) de richtlijnen van de Autoriteit Persoonsgegevens voor de rest van het incidentbeheer proces.
      ii. De incidentcoördinator, in samenwerking met de beheerorganisatie, informeert alle partijen in het DSGO en relevante partijen daarbuiten (bijv. brancheorganisaties, het NCSC of zelfs wetshandhaving) over het incident (en dat deze wordt opgelost), wie de incidentmanager is en wie de incidentcoördinator is.
      iii. De incidentcoördinator stelt een actieplan op om risico's en schade te minimaliseren.
6. **Update betrokken partijen:** De incidentcoördinator organiseert het contact met de betrokken partijen, monitort de voortgang en assisteert bij behandelen van de melding als dat nodig is. De incidentcoördinator communiceert, in samenwerking met de beheerorganisatie, de voortgang met partijen in het DSGO in het geval van een Prioriteit 1 of 2 incident.
7. **Proces afronden:** Wanneer het incident verholpen of opgelost is sluit de incidentcoördinator het proces en;
   a. In geval van een Prioriteit 3 incident licht de incidentcoördinator de betrokken partijen in dat het proces is afgerond.
   b. In geval van een Prioriteit 1 of 2 incident licht de incidentcoördinator partijen in het DSGO in dat het proces is afgerond.

8. **Evaluatie:** De incidentcoördinator evalueert samen met de beheerorganisatie de afhandeling van het incident samen met de betrokken partijen en registreert de evaluatie voor leerdoeleinde. De beheerorganisatie kan er voor kiezen om de evaluatie te delen met andere DSGO deelnemers.

# Classificatie incidenten

Voor ieder incident maakt de meldende partij een inschatting van de classificatie en de incidentcoördinator accepteert of wijzigt deze (zie Incidentbeheer voor meer details). Elk incident wordt geclassificeerd in Prioriteit 1, 2 of 3. Welke Prioriteit het incident krijgt toegewezen is afhankelijk van de geschatte impact volgens het onderstaande framework. Wanneer een incident aan minimaal een van de impact indicatoren voldoet, wordt het incident op minimaal dat niveau geclassificeerd. Deze incident classificatie is gebaseerd op de incident classificatie in iSHARE.

| Classificatie | Impact indicatoren |
|---|---|
| **Prioriteit 3 - Laag** | • Verwachte duur van minder dan 4 uur binnen het beschikbaarheidsvenster<br>• Betrokkenheid van 1 partij<br>• (Mogelijke) datalek, bijvoorbeeld door het verlies van een harde schijf, of door malware<br>• Fraude of het vermoeden van fraude, bijvoorbeeld door een werknemer of hacker |
| **Prioriteit 2 - Midden** | • Verwachte duur van meer dan 4 uur binnen het beschikbaarheidsvenster<br>• Betrokkenheid van minimaal 5 partijen<br>• Datalek met meldplicht bij de Autoriteit Persoonsgegevens<br>• Impact op vertrouwelijkheid en integriteit. |
| **Prioriteit 1 - Hoog** | • Verwachte duur van meer dan 12 uur binnen het beschikbaarheidsvenster<br>• Betrokkenheid van minimaal 10 partijen<br>• Grote impact op imago en vertrouwen van het DSGO<br>• Politieke implicaties<br>• Fundamentele juridische of technische kwetsbaarheid. |

✔ Partijen die een incident melden MOETEN de naam van de verondersteld veroorzakende partij met een onderbouwing van de constatering/vermoeden, datum, tijd, ingeschatte incident classificatie en impact op de datadienst melden bij de rapportage over een incident

✔ De incidentcoördinator MOET het incident beoordelen en legt het classificatie niveau vast

**Merk op,** de bovenstaande lijst van indicatoren is niet uitputtend.

# Handhaving

Incidenten hebben een negatieve impact op het vertrouwen in het afsprakenstelsel. Vandaar dat de beheerorganisatie alle incidenten snel en secuur afhandelt via het incidentenbeheer. Tijdens dat proces kan de beheerorganisatie besluiten om parallel een handhavingsproces te starten. Dit proces wordt gestart als er sprake is van een overtreding die volgens de beheerorganisatie mogelijk een sanctie rechtvaardigt. Een overtreding is een incident dat wordt veroorzaakt doordat een deelnemer zich niet aan de in het afsprakenstelsel opgestelde afspraken houdt. Een overtreding wordt geclassificeerd op basis van impact en risico. De beheerorganisatie kan wanneer zij dit noodzakelijk acht een van de volgende sancties opleggen bij een overtreding:

- **Waarschuwingen** zijn waarschuwende adviezen over een overtreding waarin gedeeld wordt wat moet gebeuren om de overtreding ongedaan te maken en wanneer dit gebeurd moet zijn.
- **Schorsing** is het tijdelijk op inactief zetten van een partij binnen het DSGO.
- **Uitsluiting** is het permanent verwijderen van de partij binnen het DSGO. Deze handeling bevat ook een DSGO brede melding voor informatiedoeleinden dat de partij is uitgesloten.

✔️ De beheerorganisatie MOET voordat het overgaat tot handhaven de belangen van het DSGO, de betrokken partijen en de deelnemers in overweging nemen en het doel van de maatregel afwegen tegen de gevolgen

## Doelstelling

Het doel van handhaving is het vertrouwen in het DSGO te waarborgen, evenals de vertrouwelijkheid en/of integriteit van (gegevens binnen) het DSGO netwerk te beschermen.

## Verantwoordelijkheid

Verschillende partijen hebben verantwoordelijkheden bij het handhaven.

### Beheerorganisatie

De beheerorganisatie is verantwoordelijk voor het uitvoeren van het handhavingsproces. Daarnaast is het de verantwoordelijkheid van de beheerorganisatie om de vertrouwelijkheid en/of integriteit van (gegevens binnen) het afsprakenstelsel te beschermen. Handhaving is hier een onderdeel van.

✔️ De beheerorganisatie MAG een handhavende maatregel (waarschuwing, schorsing of uitsluiting) opleggen bij een overtreding om de vertrouwelijkheid en/of integriteit van het DSGO afsprakenstelsel te beschermen

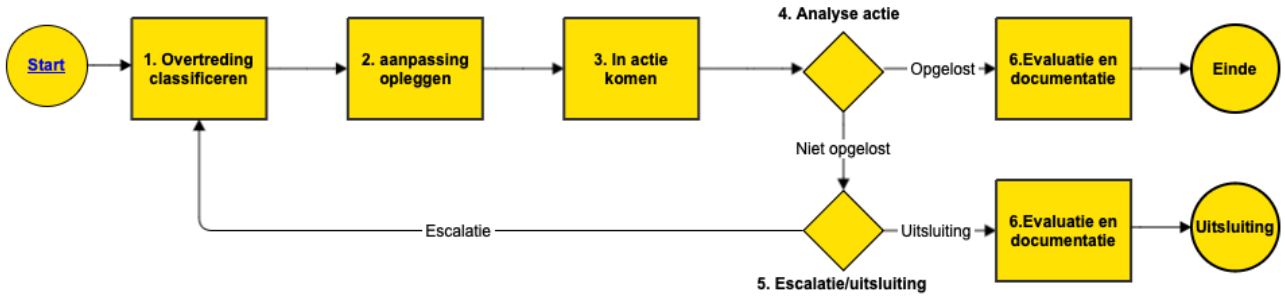
### Betrokken partijen

Iedere bij het DSGO betrokken partij heeft de verantwoordelijkheid om te allen tijde, maar vooral na het ontvangen van een waarschuwing of schorsing, te handelen in overeenstemming met de regels en richtlijnen van het afsprakenstelsel.

✔️ Partijen MOETEN te allen tijde handelen in overeenstemming met het afsprakenstelsel

# Proces

Onderstaand figuur geeft een globaal beeld van de stappen tijdens een handhavingsproces, voor meer details zie het geschreven proces onder het figuur.




Het handhavingsproces is als volgt:

**Startpunt:** Besluit start **handhavingsproces:** (Stap 4 incidentenbeheer proces) Op basis van de ingekomen melding van een incident kan de beheerorganisatie besluiten om het handhavingsproces te starten. Zie incidentbeheer voor meer informatie.

1. **Overtreding classificeren:** De beheerorganisatie beoordeelt de overtreding en wijst een de classificatie toe.
2. **Aanpassing/rectificatie opleggen:** De beheerorganisatie registreert de vermeende overtreding en;
   a. Als het geclassificeerd is als een Kleine overtreding stelt het de vermeende overtredende partij hier van op de hoogte samen met de reden(en), de noodzakelijke aanpassingen/rectificaties en binnen welke termijn deze verwerkt moeten zijn;
   b. Als het geclassificeerd is als een Middelgrote overtreding stuurt het de vermeende overtredende partij een officiële waarschuwing samen met de reden(en), de noodzakelijke aanpassing(en)/rectificatie(s) en binnen welke termijn deze verwerkt moeten zijn;
   c. Als het geclassificeerd is als een Grote overtreding schorst het de vermeende overtredende partij door de status van de betreffende partij in de registers te wijzigen naar ‘geschorst’, tot de noodzakelijke verandering(en)/rectificatie(s) zijn doorgevoerd. De beheerorganisatie communiceert de schorsing met het DSGO netwerk.
3. **Overtredende partij heeft de kans om actie te ondernemen:** De overtredende partij:
   a. Voert de aanpassing of rectificatie door binnen de gestelde tijd en informeert de beheerorganisatie over de aanpassing/rectificatie of;
   b. Stelt de beheerorganisatie binnen 5 werkdagen na ontvangst van de melding/sanctie op de hoogte van zijn bezwaar tegen de melding/sanctie waarna de beheerorganisatie hier binnen 5 werkdagen op reageert. De overtredende partij krijgt hierna 5 werkdagen om op de reactie van de beheerorganisatie te reageren (welke aanpassingen kan bevatten t.o.v. de initiële melding/waarschuwing) of;
   c. Onderneemt geen actie.
4. **Analyse van de actie:** De beheerorganisatie bepaalt of de (mogelijk genomen) actie van de overtredende partij voldoende is. Afhankelijk van de classificatie van de overtreding en (mogelijke) oplossing, kan er opnieuw actie worden ondernomen. Als de opgelegde aanpassing/rectificatie voldoende is opgevolgd binnen de gegeven tijd volgt stap 6. Als dat niet het geval is zal de beheerorganisatie:
   a. In het geval van een Kleine overtreding:
      i. De overtredende partij een waarschuwing sturen samen met de reden, de benodigde aanpassing/rectificatie en binnen welke termijn deze verwerkt moet zijn.
   b. In het geval van een Middelgrote overtreding:
      i. De overtredende partij een laatste waarschuwing sturen voordat deze geschorst wordt samen met de reden, de benodigde aanpassing/rectificatie en binnen welke termijn deze verwerkt moet zijn.
   c. In het geval van een Grote overtreding:
      i. De overtredende partij een laatste waarschuwing sturen voordat deze uitgesloten wordt samen met de reden, de benodigde aanpassing/rectificatie en binnen welke termijn deze verwerkt moet zijn.
5. **Escalatie/uitsluiting:** Als de overtredende partij de (laatste) waarschuwing blijft negeren na een redelijke termijn zal de beheerorganisatie:
   a. In geval van een Kleine overtreding:
      i. Opschalen naar een Middelgrote overtreding en terug gaan naar stap 4b.
   b. In geval van een Middelgrote overtreding:
      i. Opschalen naar een grote overtreding en terug gaan naar stap 2c.

c. In geval van een Grote overtreding:
    i. De deelname van de overtredende partij beëindigen door de deelnameovereenkomst op te zeggen;
    ii. De overtredende partij uitsluiten van het DSGO door de status van de partij in de registratie aan te passen naar ‘beëindigd’ en start de uittreding (zo veel mogelijk) in lijn met het uittredingsproces;
    iii. De uitsluiting van de overtredende partij communiceren met het DSGO netwerk. De uitgesloten partij mag voor 12 maanden niet opnieuw in een toetredingsproces participeren.

6. **Evaluatie en documentatie:** De beheerorganisatie evalueert de overtreding met de rapporterende partij en/of (een) ander(e) partij(en) en documenteert de evaluatie voor leerdoeleinden.
7. **Einde handhaving:** Overtreding is opgelost of overtredende partij is uitgesloten

# Classificatie overtredingen

Een handhavingsproces begint wanneer de beheerorganisatie in het incidentbeheer bepaalt dat het incident een overtreding is die zwaar genoeg is om een handhavingsproces te starten. Elke overtreding wordt geclassificeerd als Kleine, Middelgrote of Grote overtreding. Welke classificatie is toegewezen is afhankelijk van de geschatte impact of risico op het DSGO op basis van het onderstaande framework. Afhankelijk van de classificatie zal een vorm van handhaving worden toegepast.

| Classificatie | Impact of risico |
|---|---|
| **Kleine overtreding** | • Niet voldoen aan de vereisten van het toetredingsproces en/of;<br>• Niet voldoen aan service level agreements, en/of;<br>• Gebruiken van verlopen informatie beveiliging certificering, (bijv. ISO27001, ISAE 3402), en/of;<br>• Een klein beveiligingslek, bijvoorbeeld door het verliezen van een USB-stick, laptop, harddisk, een hackpoging of door gevonden malware, en/of;<br>• Fraude of vermoeden van fraude door bijvoorbeeld een werknemer of een hacker. |
| **Middelgrote overtreding** | • Herhaaldelijke kleine overtreding, en/of;<br>• Combinatie van kleine overtredingen, en/of;<br>• Het ernstig belemmeren van andere deelnemers, en/of;<br>• Een groot beveiligingslek of meerdere beveiligingslekken die moeten worden gerapporteerd in lijn met meldplicht datalekken, en/of;<br>• (Andere) inbreuk op de vertrouwelijkheid en integriteit van (de data* in) het DSGO afsprakenstelsel. |
| **Grote overtreding** | • Herhaaldelijke grote overtreding, en/of;<br>• Netwerk brede belemmering(en) voor andere partijen, en/of;<br>• Een (andere) inbreuk op de vertrouwelijkheid en integriteit van het gehele afsprakenstelsel. |

* Data omvatten de gegevens die worden gebruikt voor de functionaliteiten van het DSGO, maar NIET de inhoud van de datadienst.

✔️ De beheerorganisatie MOET de overtreding beoordelen en legt het classificatie niveau vast

ℹ️ **Merk op,** de bovenstaande lijst van impact en risico's is niet uitputtend.

# Change en release management

Het afsprakenstelsel is dynamisch en ontwikkelt verder om ervoor te zorgen dat het DSGO aan de eisen en behoeftes van deelnemers en belanghebbenden blijft voldoen. Indien nodig, kunnen afspraken worden toegevoegd, gewijzigd, of verwijderd. Om de impact van wijzigingen te minimaliseren, is een gecontroleerde change en release management proces vastgelegd.

Het change en release management proces gaat over wijzigingen in het afsprakenstelsel. Het gaat niet  niet over de wijzigingen en releases van datadiensten of voorzieningen. Mogelijk leiden de wijzigingen in het afsprakenstelsel tot impact op datadiensten en voorzieningen waarvoor zijn updates nodig zijn om conform de wijzigingen in het afsprakenstelsel te blijven handelen.

## Doelstelling

Change en release management van het afsprakenstelsel heeft als doelstelling dat het DSGO toekomstbestendig is en meebeweegt met de wensen en eisen van haar deelnemers en belanghebbenden. Omdat afspraken gelden tussen deelnemers en belanghebbenden, dient een eerlijke, representatieve en inclusieve vertegenwoordiging zeggenschap over wijzigingen van het afsprakenstelsel te hebben. Het change en release management proces ondersteunt twee doelstellingen:

- Op transparante en zorgvuldige wijze besluiten welke wijzigingen wel of niet worden doorgevoerd. Hierbij hebben de deelnemers en belanghebbenden invloed op de wijzigingen, en deelnemers inspraak in de wijzigingen.
- Releases van wijzigingen worden op een gestandaardiseerde wijze doorgevoerd met minimale impact en verstoring in de werking van het DSGO.

## Verantwoordelijkheid

Verschillende partijen die gebruikmaken van het afsprakenstelsel hebben een verantwoordelijkheid in change en release management.

### Beheerorganisatie

De beheerorganisatie bestaat uit meerdere organen zoals beschreven in de governance. Verschillende organen zijn betrokken bij het change en release management proces.

- De beheerorganisatie is verantwoordelijk voor het faciliteren van het change en release management proces volgens de procesbeschrijving. Verder mag de beheerorganisatie een verzoek voor wijzigingen indienen.
- De gebruikersraad is verantwoordelijk voor het schetsen van de strategische kaders voor de inhoudelijke doorontwikkeling van het DSGO. Binnen die kaders vindt change en release management  plaats. Daarmee heeft de gebruikersraad geen rol in het proces zelf.
- De change advisory board is verantwoordelijk voor het adviseren van de beheerorganisatie in de ingediende veranderingen.

✔️ De beheerorganisatie MOET het change en release management proces begeleiden

✔️ De beheerorganisatie MAG een Request For Change (RFC) indienen conform het change en release management proces

✔️ De change advisory board MOET de beheerorganisatie adviseren in de behandeling van Requests For Change (RFCs)

### Deelnemers

Iedere deelnemer heeft inspraak in de doorontwikkeling van het afsprakenstelsel. Een deelnemer kan een verzoek voor wijzigingen indienen, en heeft recht heeft op inspraak bij de (door)ontwikkeling van het afsprakenstelsel. Deelnemers recht hebben op representatie in

de Change Advisory Board, en daarmee inspraak op het adviseren van de beheerorganisatie in de ingediende veranderingen.

✔ Deelnemers MOGEN een Request For Change (RFC) indienen conform het change en release management proces

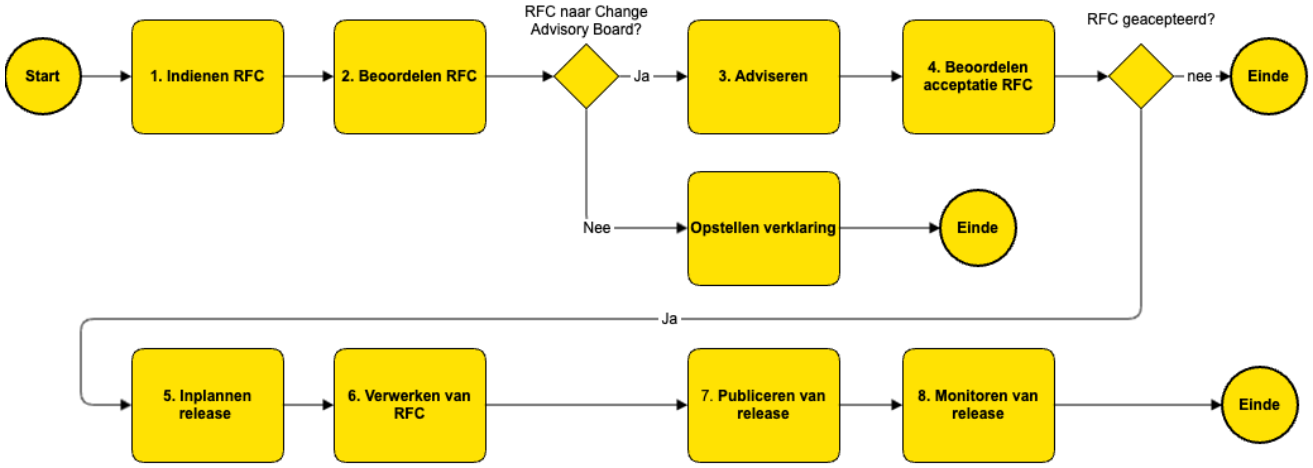
### Belanghebbenden die geen deelnemers zijn

Er zijn ook partijen die wel belanghebbende zijn, maar (nog) geen deelnemers. Dit zijn bijvoorbeeld partijen die in het proces zitten om deelnemer te worden, of de rollen rechthebbende en datadienstgebruikers hebben. Deze partijen mogen een verzoek voor wijzigingen indienen.

✔ Partijen MOGEN een Request For Change (RFC) indienen conform het change en release management proces

## Change en Release Management Proces

Onderstaand figuur geeft een globaal beeld van de stappen in het change en release proces, deze wordt in detail beschreven onder het figuur.




Het change en release proces is als volgt:

1. **Indienen Request for Change (RFC)**: een of meerdere partijen dienen een RFC in bij de beheerorganisatie. Een RFC bevat minimaal het volgende:
   - een beschrijving van de concrete gewenste wijziging,
   - een beschrijving van de aanleiding/onderbouwing waarom deze wijziging gewenst is,
   - een indicatie hoe urgent en belangrijk deze wijziging is,
   - een potentiële oplossing of oplossingsrichting,
   - een Indicatie van de verwachte impact op het afsprakenstelsel en datadienstaanbieders, datadienstgebruikers, rechthebbenden, marktvoorzieningen, stelselvoorzieningen,
   - een rechtvaardiging van de wijziging, al dan niet inclusief business case. De toegevoegde waarde van de wijziging moet duidelijk zijn.

   De beheerorganisatie neemt de RFC op en zorgt dat deze gelogd is zodat ingediende RFCs altijd op een later moment herproduceerbaar zijn.
2. **Beoordelen RFC**: de beheerorganisatie stelt de haalbaarheid en de impact van de ingediende RFC vast. Hierin neemt de beheerorganisatie de richtinggevende principes en scope van het DSGO in mee. Er zijn twee mogelijke uitkomsten:
   a. De RFC wordt besproken in een meeting met het change advisory board. De beheerorganisatie informeert vooraf de change advisory board en de indienende partij(en) over wanneer de RFC ingepland staat ter bespreking.
   b. De RFC wordt niet besproken in een meeting met de change advisory board. De beheerorganisatie stelt een schriftelijke reactie op waarom is besloten om de RFC (in de huidige status) niet voor te leggen aan de change advisory board.

3. **Adviseren:** De change advisory board krijgt voldoende tijd om de RFC te beoordelen en adviseert de beheerorganisatie hoe om te gaan met de RFC.
4. **Beoordelen acceptatie RFC**: De beheerorganisatie bepaald met het advies van de change advisory board (op basis van o.a. het voorstel van de oplossing en een geschatte impact):
   a. of de RFC geaccepteerd wordt en met welke prioriteit deze wordt doorgevoerd
   b. of de RFC verworpen wordt
   De beheerorganisatie komt met een schriftelijke verklaring naar de change advisory board en de indienende partij(en), waarin wordt uitgelegd waarom de RFC is geaccepteerd of verworpen, en wat de prioriteit van de release van de RFC is mits hij geaccepteerd is.
5. **Inplannen release**: Als de RFC geaccepteerd is, update de beheerorganisatie de release kalender en de prioriteiten.
6. **Verwerken van RFC**: De beheerorganisatie is verantwoordelijk voor het correct verwerken van de wijzigingen in het afsprakenstelsel.
   - Mochten de wijzigingen in het afsprakenstelsel leiden tot nodige aanpassingen in het DSGO, dan is de beheerorganisatie verantwoordelijk om de desbetreffende deelnemers en belanghebbenden hierover te informeren. Het moet voor de deelnemers en belanghebbenden bekend zijn wanneer de release verwacht wordt en per wanneer zij moeten voldoen aan de doorgevoerde release.
7. **Publiceren release**: De beheerorganisatie publiceert een nieuwe versie van het afsprakenstelsel conform versie richtlijnen. Wanneer er een update heeft plaatsgevonden, dan is de beheerorganisatie verantwoordelijk dat deelnemers en belanghebbenden hiervan op de hoogte zijn.
8. **Monitoren van release**: De beheerorganisatie monitort de release en voorziet deelnemers en belanghebbende van support om te kunnen voldoen aan de afspraken uit de release indien nodig. De mate en hoe dit gebeurd is afhankelijk van de aard van de wijziging en de doorlooptijd om hieraan te voldoen.

## Uitzonderingen

### Spoedwijzigingen

Spoedwijzigingen zijn wijzingen die zo snel mogelijke geïmplementeerd moeten worden. Spoedwijzigingen zijn wijzigingen die of betrekking hebben op een prioriteit 1 (hoog) incident die gericht is aan de beheerorganisatie, of wanneer dit impact heeft op de werking van het DSGO kan hebben als de spoedwijziging niet doorgevoerd wordt. In dat geval, mag de beheerorganisatie het change en release management proces versnellen. Zij kan kiezen om leden van de change advisory board ad-hoc te consulten over de wijzigingen, mits de timing het toelaat en noodzakelijk wordt geacht. Achteraf moet de beheerorganisatie de change advisory board alsnog volledig informeren over de wijziging.

✔️ De beheerorganisatie MAG in het geval van spoed besluiten om af te wijken van het standaard change en release proces

### Kleine wijzigingen

Kleine wijzigingen die geen impact hebben op de technische werking of juridische basis van het DSGO mogen ook zonder het doorlopen van het change en release proces plaatsvinden. Dit zijn bijvoorbeeld herstructurering van de inhoud, verbeteren van taalfouten of updates in hyperlinks en labels.

✔️ De beheerorganisatie MAG in het geval van een kleine wijziging, die geen impact heeft op de technische werking of juridische basis, deze uitvoeren zonder het standaard change en release proces te doorlopen

# Versie richtlijnen

Elke versie van het afsprakenstelsel heeft een uniek identificerend kenmerk die betekenis geeft over de significantie van de wijziging. Het afsprakenstelsel gebruikt een nummering van drie cijfers voor de versienummering (a.b.c.). Afhankelijk van de wijzigingen die in het afsprakenstelsel worden doorgevoerd worden verschillende elementen van het versienummer verhoogt:

1. Grote wijziging: De “a” wordt gewijzigd voor een significante of niet terug te draaien wijziging (van v1.0 naar v2.0)
2. Kleine wijziging: De “b” wordt gewijzigd voor reguliere wijzigingen of nieuwe functionaliteit (van v1.2 naar v1.3)
3. Verbetering: De “c” wordt gewijzigd voor kleine verbeteringen (van v1.2 naar v1.2.1)

De beheerorganisatie kan ervoor kiezen om meerdere stappen in een kleine wijziging tegelijk te maken (van v1.2 naar v1.5) om aan te geven dat er significante wijzigingen zijn gemaakt, maar niet genoeg om een grote wijziging aan te geven.

✔️ De beheerorganisatie MOET bij een release van het afsprakenstelsel de wijziging van versienummer bepalen

✔️ De beheerorganisatie MOET releases communiceren middels de versie richtlijnen

# Marktvoorzieningen

Voorzieningen zijn ondersteunende faciliteiten die nodig zijn voor het functioneren van het DSGO. Marktvoorzieningen zijn voorzieningen die geleverd worden door partijen in de gebouwde omgeving. Op dit moment worden twee marktvoorzieningen verwacht in het DSGO. Authenticatiediensten en autorisatieregisters. Het DSGO volgt iSHARE in de implementatie van alle marktvoorzieningen.

✔️ Authenticatiediensten MOETEN voldoen aan alle eisen van een Identity Provider volgens iSHARE

✔️ Autorisatieregisters MOETEN voldoen aan alle eisen van een Autorization Registry volgens iSHARE

# Stelselvoorzieningen

Voorzieningen zijn ondersteunende faciliteiten die nodig zijn voor het functioneren van het DSGO. Stelselvoorzieningen zijn voorzieningen die worden geleverd door de beheerorganisatie en ondersteunen partijen in de voorbereiding op en bij de uitvoering van datadiensten. Momenteel worden drie stelselvoorzieningen voorzien, de conformiteitstest-tool, het developer portal en de stelselcatalogus. Wanneer de eerste functionaliteiten van stelselvoorzieningen bruikbaar zijn worden deze beschikbaar gesteld.

**Merk op,** Op dit moment zijn de eerste prototypes van de stelselvoorzieningen in ontwikkeling. Deze prototypes zijn ontwikkeld om op kleine schaal eerste ervaring op te doen als basis voor de ontwikkeling van volwassen stelselvoorzieningen.

## Developer portal

De developer portal is een online interface waar ontwikkelaars documentatie tools en middelen kunnen vinden om effectief de DSGO componenten van een datadienst te implementeren, waardoor ze snel en goed softwaretoepassingen kunnen bouwen en integreren. Het prototype developer portal biedt ontwikkelaars interactieve documentatie waarin de componenten van datadiensten die gespecificeerd zijn in het afsprakenstelsel, inclusief methodes en responseformaten waar van toepassing, duidelijk zijn omschreven. Het stelt gebruikers in staat om direct in de portal API-calls te testen zonder externe tools. Daarmee is het een centrale plek waar ontwikkelaars bronnen, voorbeelden en best practices kunnen vinden om datadiensten effectief te implementeren.

Bekijk hier de meest recente publieke versie van het prototype developer portal

**Merk op,** de prototype stelselcatalogus is nog in ontwikkeling. Wanneer deze wordt bijgewerkt, zal hier meer informatie over de functionaliteiten van de developer portal te vinden zijn.

## Conformiteitstest-tool

De conformiteitstest-tool (CTT) is een software hulpmiddel dat is ontworpen om de beheerorganisatie te laten verifiëren of de implementatie van APIs voldoet aan het afsprakenstelsel. Het prototype richt zich op het valideren van generieke afspraken voor DSGO datadienstimplementaties van datadienstaanbieders.

Bekijk hier de meest recente publieke versie van het prototype conformiteitstest-tool

**Merk op,** de prototype CTT is nog in ontwikkeling. Wanneer deze wordt bijgewerkt, zal hier meer informatie over het (aanvragen van) gebruik van de (prototype) CTT te vinden zijn.

## Stelselcatalogus

De stelselcatalogus biedt zichtbaarheid van datadiensten in het DSGO, zowel voor mensen (website) als machines (via datadiensten). De stelselcatalogus biedt een overzicht van datadienstaanbieders en datadiensten in het DSGO om gebruikers de benodigde informatie te bieden voor het vinden en uitvoeren van datadiensten. De prototype stelselcatalogus zal datadienstaanbeiders en de bijbehorende datadiensten bevatten die in ontwikkeling zijn binnen de adoptieprojecten uit het DSGO programma. In een toekomstige versie kan de stelselcatalogus ook informatie over marktvoorzieningen bevatten.

Bekijk hier de meest recente publieke versie van het prototype stelselcatalogus

**Merk op,** de prototype stelselcatalogus is nog in ontwikkeling. Wanneer deze wordt bijgewerkt, zal hier meer informatie over het functioneren van de stelselcatalogus te vinden zijn.

# Specifieke afspraken

In dit hoofdstuk worden de specifieke afspraken die van toepassing zijn op datadiensten gepresenteerd.

- BIM in datadiensten

In de introductie zijn de aanleiding en doel van het DSGO, en de richtinggevende principes van het afsprakenstelsel gepresenteerd. In de kern van het afsprakenstelsel zijn datadiensten, het rollenmodel en de ondersteunende functionaliteiten die deel uitmaken van het DSGO geïntroduceerd. Generieke afspraken zijn data agnostisch en van toepassing voor alle datadiensten zijn gepresenteerd.

Op dit moment is het afsprakenstelsel in ontwikkeling binnen het DSGO-programma. In een toekomstige versie van het afsprakenstelsel zal dit hoofdstuk worden doorontwikkeld.

# BIM in datadiensten

**Merk op,** deze specifieke afspraken komen voort uit de BIM-vergunningen use case binnen het DSGO programma.

Op veel verschillende plekken van de waardeketen van de gebouwde omgeving wordt Building Information Modelling (BIM) gebruikt. ISO 19650 is de internationale norm voor het beheer van informatie over de gehele levenscyclus van een bouwwerk, en definieert BIM als het gebruik van een gedeelde digitale representatie van een bouwwerk om ontwerp-, bouw- en gebruiksprocessen te faciliteren en een betrouwbare basis te vormen voor besluitvorming. Volgens ISO 19650 wordt informatie gestructureerd in informatie containers, welke informatie relevant voor BIM kan bevatten. Wanneer men spreek over een BIM-model, wordt typisch een informatie container met gestructureerde geometrische modellen bedoeld.

✔ Als datadiensten gebruik maken van gestructureerde geometrische modellen (een BIM-model) dan MOETEN partijen alle `DSGO.BIM` afspraken volgen

Er bestaan op dit moment een groot aantal variaties in de semantische modellen die gebruikt worden voor BIM-modellen. In het DSGO worden een aantal aspecten voor het gebruik van BIM-modellen in een datadienst gestandaardiseerd met specifieke afspraken die in lijn zijn met de richtinggevende principes.

Deze specifieke afspraken gelden voor alle datadiensten binnen de waardeketen van de gebouwde omgeving zoals vastgelegd door de GEBORA (GEBouwde Omgeving Referentie Architectuur)

:Quotes:

**Bron:** Gebouwde Omgeving Referentie Architectuur - NORA online

We onderkennen vooralsnog 6 ketens: (1) registreren, vergunning, toezicht houden en handhaven (2) eigendom en gebruiksrechten (3) plannen, ontwerpen en realiseren (4) beheren en instandhouden (5) exploiteren en gebruiken en (6) inwinnen, produceren, opslaan, verkopen en transporteren van producten, materieel, materiaal en medewerkers.

De afspraken op deze pagina worden verder gedetailleerd voor gespecificeerde contexten:

- BIM voor vergunning of melding afhandelen
  - BIM voor vergunning of melding afhandelen voor gebouwen met als gebruiksfunctie woonfunctie

Het DSGO volgt in deze specifieke afspraken het gebruik van Industry Foundation Classes (IFC) zoals vastgelegd in de open standaarden van buildingSMART International en overgenomen in ISO 16739. Hiervoor wordt gezorgd dat elk BIM-model wat volgens het DSGO gedeeld wordt binnen een datadienst, dezelfde semantische standaard moet aanhouden.

✔ `DSGO.BIM`: Datadienstaanbieders ZOUDEN IFC4 ADD2 TC1 (v4.0.2.1) MOETEN ondersteunen

**Merk op,** er is in het DSGO gekozen voor de buildingSMART International IFC4 ADD2 TC1 (v4.0.2.1) omdat omdat deze onderandere naukeurige geo-referentie mogelijkheden bevat ten opzichte van andere open alternatieven zoals de IFC2x3 TC1 (versie 2.3.0.1)

De ondersteuning voor georeferentie in IFC2x3 bied enkel mogelijkheden voor het definiëren van de locatie en de oriëntatie van het gebouw ten opzichte van de wereldcoördinaten. Het gebruikte voornamelijk het `IfcSite` en `IfcBuilding` entiteiten voor deze doeleinden, en had een beperkte set attributen om geo-referentie-informatie te definiëren. IFC4 introduceerde verbeterde ondersteuning voor geo-referentie, met meer gedetailleerde en uitgebreide mogelijkheden om locatie-informatie en geospatiale data te specificeren. Het introduceerde bijvoorbeeld de `IfcMapConversion` en `IfcProjectedCRS` entiteiten die samenwerken om een gedetailleerd georeferentie-informatiesysteem op te zetten. Met deze verbeteringen in IFC4 kunnen gebruikers de geografische

positie, de oriëntatie en de schaal van het model ten opzichte van een kaartprojectiesysteem op een veel gedetailleerdere manier specificeren dan in IFC2x3.

Information Delivery Specifications (IDS) is een open standaard van buildingSMART International en specifiek bedoeld voor het vastleggen van aanlever- en uitwisseleisen aan BIM IFC modellen. De afspraak in het DSGO betreft aanlevereisen (bijvoorbeeld, het IFC4 model moet een bepaald informatie component of entiteit bevatten (vb: IfcSpace/IfcSensor/IfcDoor etc.) met een bepaald attribuut ObjectType (functie)) en niet de inhoudelijke eisen vanuit regelgeving (bijvoorbeeld een scheidingswand tussen twee brandcompartimenten dient 60 minuten weerstand te bieden bij brand doorslag en overslag). Verder biedt IDS geen ondersteuning voor geometrische vereisten of het in kaart brengen van vereisten met projectprocessen, vandaar dat de afspraak enkel van toepassing is ‘indien IDS het technisch toe laat’.

✔️ `DSGO.BIM`: Datadienstaanbieders ZOUDEN aanlevereisen aan een IFC4 model MOETEN specificeren met IDS v0.9.6 indien IDS het technisch toe laat

**Merk op,** de buildingSMART International IDS standaard is op dit moment in ontwikkeling. Het is de verwachting dat richting het einde van 2023 er een v1.0 van de IDS wordt gepubliceerd. Deze ontwikkelingen worden in de gaten gehouden, en deze afspraak zal worden geüpdate indien relevant. IDS v0.9.6 is de meest volwassen versie op het moment van schrijven.

**Merk op,** er is in het DSGO gekozen voor de buildingSMART International IDS op basis van de literatuur (bron), en dat dit inlijn is met de richtinggevende principes:

‘IDS has been identified as the most advantageous method, when it comes to automated compliance checking by validation of the alphanumerical IR’.

# BIM voor vergunning of melding afhandelen

**Merk op,** deze specifieke afspraken komen voort uit de BIM-vergunningen use case binnen het DSGO programma.

In de GEBORA is de waardeketen 01 voor Registratie, Vergunning, Toezicht en Handhaving vastgelegd. Hierin vindt de Fase 01.02 Vergunning of Melding Afhandelen plaats. In het DSGO worden de afspraken voor BIM in datadiensten nog verder gespecificeerd in deze context.

**Merk op,** de GEBORA wordt binnenkort gepubliceerd. Wanneer deze beschikbaar is zal deze pagina worden bijgewerkt met een link naar de bron.

✔️ Als datadiensten gebruikt worden in de Fase 01.02 Vergunning of Melding Afhandelen, en gebruik maken van gestructureerde geometrische modellen (een BIM-model) dan MOETEN partijen alle `DSGO.BIM.Vergunning` afspraken volgen

✔️ `DSGO.BIM.Vergunning`: Datadienstaanbieders MOETEN IFC4 ADD2 TC1 (v4.0.2.1) ondersteunen

✔️ `DSGO.BIM.Vergunning`: Datadienstaanbieders MOETEN aanlevereisen met IDS v0.9.6 beschrijven indien IDS het technisch toe laat

De afspraken op deze pagina worden verder gedetailleerd voor gespecificeerde contexten:

- BIM voor vergunning of melding afhandelen voor gebouwen met als gebruiksfunctie woonfunctie

# BIM voor vergunning of melding afhandelen voor gebouwen met als gebruiksfunctie woonfunctie

**Merk op,** deze specifieke afspraken komen voort uit de BIM-vergunningen use case binnen het DSGO programma.

Binnen waardeketen Fase 01.02 worden (o.a.) vergunningen aangevraagd voor gebouwen met als gebruiksfunctie woonfunctie. Wanneer in deze context BIM-modellen worden gedeeld in een datadienst gelden de afspraken op deze pagina. Deze afspraken bouwen voort op de afspraken voor BIM in datadiensten voor vergunning of melding afhandelen in deze precieze context. Een gebouw met een woonfunctie (volgens het Informatiepunt Leefgomgeving) is gebouw waar een onderdeel van wordt gebruikt om te wonen. Dat wil zeggen dat het adres als woonadres in de gemeentelijke basisadministratie staat.

✔️ Als datadiensten gebruikt worden in de Fase 01.02 Vergunning of Melding Afhandelen, en gebruik maken van gestructureerde geometrische modellen (een BIM-model) voor een gebouw met een woonfunctie dan MOETEN partijen alle `DSGO.BIM.Vergunning.Woonfunctie` afspraken volgen

## Georeferentie

Het is voor alle betrokkenen (bv projectontwikkelaars en gemeentes) essentieel om het ontwerp te kunnen relateren aan een plek in de fysieke wereld. Daarvoor moet de ontvanger van een BIM-model weten welk coördinatenstelsel gebruikt is. Volgens Geonovum's Handreiking Gebruik coördinaatreferentiesystemen bij uitwisseling en visualisatie van geo-informatie, wordt hier het Rijksdriehoeksstelsel voor gebruikt. Dit is het nationale geprojecteerde coördinatensysteem. Naast de x en y coördinaat in het `RD_new` stelsel, is de hoogte t.o.v. NAP ook van belang, al is de peilhoogte in projecten soms pas laat bekend. Er is gekozen om zowel EPSG:7415 als EPSG:28992 te gebruiken vanwege het belang de peilhoogte (in EPSG:7415) en de brede adoptie van EPSG:28992. Binnen IFC is IFCClass:IfcProjectedCRS speciaal voor verwijzingen naar coördinatensystemen toegevoegd in de overgang naar IFC4.

✔️ `DSGO.BIM.Vergunning.Woonfunctie`: Datadienstaanbieders MOETEN ondersteunen dat het lokale nulpunt een verwijzing bevat naar het Rijksdriehoeksstelsel ( `RD_new` ) en de hoogte t.o.v. NAP, door bij `IFCClass:IfcProjectedCRS` de waarde `Name:EPSG:7415` te gebruiken of `Name:EPSG:28992` en als Z-waarde de hoogte tegenover NAP te gebruiken

`IFCMAPCONVERSION` is binnen IFC de meest nauwkeurige & gebruikelijke plek om coördinaten door te geven. De volgende afspraak borgt dat de drie benodigde coördinaten in ieder geval ingevuld zijn. Schaal en rotatie zijn ook vaak van belang en worden mogelijk in een latere versie toegevoegd.

✔️ `DSGO.BIM.Vergunning.Woonfunctie`: Datadienstaanbieders MOETEN ondersteunen dat het BIM-model de `IFCClass:IFCMAPCONVERSION` bevat met attributen `Eastings`, `Northings` en `OrthogonalHeight` ingevuld

## Bouwlaagnaamgeving

Het specificeren van bouwlagen naamgeving voorkomt onduidelijkheid, bijvoorbeeld over wat de 1e verdieping is (begane grond, of de verdieping daarboven). De BIM Basis ILS specificeert bouwlaagnaamgeving (gebaseerd op de RVB BIM Specificaties v1.1-c paragraaf 2.1.9). Binnen IFC is `IFCBUILDINGSTOREY` de class die gemaakt is voor bouwlaagnaamgeving.

✔️ `DSGO.BIM.Vergunning.Woonfunctie`: Datadienstaanbieders MOETEN ondersteunen dat de bouwlagen gedefinieerd worden met `IFCClass:IFCBUILDINGSTOREY` en `attribuut Name` volgens de bouwlaagnaamgevingsmethode van de BIM basis ILS v2

✔️

`DSGO.BIM.Vergunning.Woonfunctie`: Datadienstaanbieders MOETEN ondersteunen dat elk geometrisch object (bv. `IfcSpace`) een relatie heeft met een bouwlaag via `IFCRELAGGREGATES` met een element uit `IFCClass:IFCBUILDINGSTOREY`

## Oppervlaktes en ruimten

Zowel voor projectontwikkelaars als voor gemeentes zijn de oppervlakten en ruimten van een gebouw nodig om bijvoorbeeld een kosten-batenanalyse te maken of een bestemmingsplantoets te doen. NEN2580 definieert een norm voor het bepalen van oppervlakten en ruimten van gebouwen. Hieronder volgen afspraken voor hoe Bruto Vloeroppervlak (BVO), Gebruiksoppervlak (GO) en Netto Vloeroppervlak (NVO) te specificeren in BIM-modellen. Naast BVO, GO en NVO zijn ook andere NEN2580 normen van belang, deze worden mogelijk in een latere versie toegevoegd.

✔️ `DSGO.BIM.Vergunning.Woonfunctie`: Datadienstaanbieders MOETEN ondersteunen dat het BIM-model de NEN2580 normen voor oppervlakken (BVO/GO) en ruimte (NVO) bevat

`IfcSpatialZone` wordt gebruikt voor BVO en GO omdat deze entiteit breder is en gebruikt kan worden om verschillende zones of gebieden in een gebouw of op een locatie te definiëren. `IfcSpatialZone` kan dus ruimten en elementen groeperen. Dit maakt het geschikt om het BVO of het GO te berekenen, aangezien dit oppervlaktes omvat die ook delen van de bouwconstructie zoals muren en kolommen bevatten. Binnen IFC is voor BVO en GO geen geschikt type gedefinieerd waardoor gekozen is voor `USERDEFINED`.

✔️ `DSGO.BIM.Vergunning.Woonfunctie`: Datadienstaanbieders MOETEN ondersteunen dat het brutovloeroppervlak (BVO) beschreven wordt als `IFCClass:IfcSpatialZone` met predefined type `USERDEFINED` met attributen uit onderstaande tabel

| **Attribuut in `IfcSpatialZone`** | | **Beschrijving** |
|---|---|---|
| `Name` | Optioneel | Vrij te kiezen ruimte nummer, bijvoorbeeld: O.12 |
| `ObjectType` | Verplicht | MOET gelijk zijn aan “BVO” |
| `LongName` | Optioneel | Vrij te kiezen tekst, bijvoorbeeld: oostvleugel laagbouw |
| `Description` | Optioneel | Vrij te kiezen tekst omschrijving, bijvoorbeeld: sociale woningen |

✔️ `DSGO.BIM.Vergunning.Woonfunctie`: Datadienstaanbieders MOETEN ondersteunen dat het gebruiksoppervlak (GO) beschreven wordt als `IFCClass:IfcSpatialZone` met predefined type `USERDEFINED` met attributen uit onderstaande tabel

| **Attribuut in `IfcSpatialZone`** | | **Beschrijving** |
|---|---|---|
| `Name` | Optioneel | Vrij te kiezen ruimte nummer, bijvoorbeeld: 1-003 |
| `ObjectType` | Verplicht | MOET gelijk zijn aan “GO” |
| `LongName` | Optioneel | Vrij te kiezen ruimte tekst, bijvoorbeeld: Penthouse |
| `Description` | Optioneel | Vrij te kiezen ruimte omschrijving, bijvoorbeeld: Hoek appartement met uitzicht op haven |

Voor NVO wordt `IfcSpace` gebruikt, wat typisch gebruikt wordt om ruimtes binnen een gebouw te definiëren. Het is bedoeld om een specifieke ruimte in het gebouw te representeren zoals een kamer, gang of liftschacht. Omdat `IfcSpace` de daadwerkelijke bruikbare ruimte binnen de muren, vloeren en plafonds van die specifieke ruimte representeert kan het worden gebruikt om de bouwbesluitfuncties te beschrijven en NVO te berekenen. De waardes in onderstaande tabel zijn gekozen zodat ze in lijn zijn met de Basis ILS, ILS O&E en RVB BIM norm ondanks dat dit afwijkt van de opbouw van de tabellen bij de twee voorgaande afspraken. Binnen IFC is voor NVO geen geschikt type gedefinieerd waardoor gekozen is voor `USERDEFINED`.

✔️ `DSGO.BIM.Vergunning.Woonfunctie`: Datadienstaanbieders MOETEN ondersteunen dat het nettovloeroppervlak (NVO) beschreven wordt als `IFCClass:IfcSpace` met onderstaande tabel

| Attribuut in `IfcSpace` | | Beschrijving |
|---|---|---|
| `Name` | Optioneel | Vrij te kiezen ruimte nummer, bijvoorbeeld: 1.12 of B_S_123.21 |
| `ObjectType` | Verplicht | MOET waarde uit ruimtefunctie bevatten, gedefinieerd volgens RVB BIM specificities tabblad: Ruimtefunctie, bijvoorbeeld: verblijfsruimte, verkeersruimte |
| `LongName` | Verplicht | MOET gelijk zijn aan “NVO” |
| `Description` | Optioneel | Vrij te kiezen ruimte tekst, bijvoorbeeld: kantoorruimte Hans |

## Groepering ruimtes

Door ruimtes te groeperen in zones, kunnen eigenschappen of attributen die gemeenschappelijk zijn voor alle ruimtes in die zone efficiënter worden beheerd. Om aan die behoefte te voldoen, is binnen de IFC-standaard `IfcZone` ontworpen waarmee `IfcSpaces` gegroepeerd kunnen worden onder één overkoepelende eenheid. Afhankelijk van de behoeften van een project kunnen zones worden gecreëerd op basis van functionele vereisten, verhuurbare eenheden, eigendomsgrenzen of andere criteria. Daarnaast wordt het eenvoudiger om specifieke delen van een gebouw te isoleren voor visualisatie of analyse. In het kader van de context van vergunningsverlening voor gebouwen met een woonfunctie, is hier gekozen om ‘woonfunctie’ als ObjectType verplicht te stellen. Daarmee wordt de relatie gelegd tussen ruimten in een BIM-model en zowel de bouwbesluitfunctie als het bestemmingsplan.

✔️ `DSGO.BIM.Vergunning.Woonfunctie`: Datadienstaanbieders MOETEN ondersteunen dat ruimten (`IfcSpaces`) die bij dezelfde wooneenheid horen, gegroepeerd worden met een `IFCClass:IfcZone` met attributen uit onderstaande tabel

| Attribuut in `IfcZone` | | Beschrijving |
|---|---|---|
| `Name` | Optioneel | Vrij te kiezen naam, bijvoorbeeld: huisnummer, bouwnummer |
| `ObjectType` | Verplicht | MOET gelijk zijn aan “woonfunctie” |
| `LongName` | Optioneel | Vrij te kiezen tekst als informatieve omschrijving |
| `Description` | Optioneel | Vrij te kiezen tekst, bijvoorbeeld: Woning van Lex |

## Voorbeeld

In lijn met de afspraken voor `DSGO.BIM.Vergunningen`, moeten de indieningsvereiste zoals geformuleerd in `DSGO.BIM.Vergunning.Woonfunctie` afspraken beschikbaar worden gesteld als IDS. Ter illustratie, hieronder een voorbeeld van een human-readable en machine-readable format van een IDS die de `DSGO.BIM.Vergunning.Woonfunctie` eisen bevat.

Human-readable: 231026-DSGO.BIM.Vergunningen.Woonfunctie.pdf

Machine-readable: 231026-DSGO.BIM.Vergunningen.Woonfunctie.ids

# Appendix

De appendix bevat extra informatie en context waar in het afsprakenstelsel aan wordt gerefereerd.

- Overzicht van conceptafspraken
- Begrippenlijst (glossary)
- FAQ

# Overzicht van conceptafspraken

Voor een overzicht van de notatieconventies gebruikt in de eisen zie deze pagina. Dit overzicht van afspraken is ook beschikbaar als een excel sheet, klik hier om deze te downloaden. Merk op, dit overzicht van afspraken is geen vervanging van het afsprakenstelsel. In het afsprakenstelsel wordt de context en onderbouwing van de afspraken duidelijk gemaakt.

## Generieke afspraken

### Generieke technische standaarden

#### RESTful API's

- ✅ Partijen ZOUDEN RESTful architectuurprincipes MOETEN volgen voor API's
- ✅ Partijen MOETEN uitsluitend standaard HTTP-operaties ondersteunen (GET, PUT, POST, PATCH, DELETE)
- ✅ Partijen MOGEN NIET de state van de client bij houden
- ✅ Partijen MOETEN data als resources beschikbaar stellen in een datadienst
- ✅ Partijen MOETEN resources een zelfstandig naamwoord in het meervoud als naam geven

---

#### HTTP(s)

- ✅ Partijen MOETEN in de context van datadiensten communiceren via het HTTP procotol
- ✅ Partijen MOETEN HTTP-headers van 100K lengte accepteren
- ✅ Partijen MOETEN bij het ontvangen van een HTTP-verzoek antwoorden met (onder andere) een statuscode die het resultaat van het verzoek aangeeft
- ✅ Partijen MOETEN geschikte HTTP-statuscodes ondersteunen die passen bij de dienst. Tenminste de volgende: 2XX, 4XX en 5XX
- ✅ Partijen ZOUDEN de standaard foutmeldingen van de HTTP 400 en 500 statuscode reeksen MOETEN ondersteunen volgens RFC 9110

---

#### JSON

- ✅ Partijen MOETEN JSON gebruiken voor het sturen van gegevens in de context van datadiensten

---

### UTC

- ✅ Partijen MOETEN alle datums en tijdstippen vastgelegd in de generieke technische standaarden van het afsprakenstelsel DSGO communiceren in UTC-tijd
- ✅ Partijen MOETEN alle datums en tijdstippen vastgelegd in de generieke technische standaarden van het afsprakenstelsel DSGO formatteren volgens het UNIX timestamp

---

## API specifications

### Generic API requirements

- ✅ Parties MUST validate that all received API calls conform to the trust framework API requirements
- ✅ Parties MUST validate that all responses to API calls conform to the trust framework API requirements
- ✅ Parties MUST define the default base URL of API endpoints following the `<domain-name>/<path>/resources` format, where `<domain-name>` is server specific and `<path>` is an optional URL path
- ✅ Parties MUST define the default base URL of API endpoints without a trailing slash
- ✅ Parties SHOULD limit API responses to include only a reasonably sized amount of data
- ✅ Parties MUST NOT include HTTP bodies in GET or DELETE requests
- ✅ Parties MAY include query options for functionalities such as filter, sort, and page in their API endpoint as defined in OData 4.01
- ✅ Parties MUST reject any requests that contain unsupported url parameters with a `501 Not Implemented` as defined in OData 4.01
- ✅ Parties MUST make caching explicit to API users
- ✅ Parties MUST include the following headers in the API response when it is not cacheable:
  `cache-control: no-store`
  `pragma: no-cache`
- ✅ Parties MUST include the following headers in the API response when it is cacheable:
  `cache-control: max-age=31536000`
  Note: `max-age` MAY vary

---

### Common endpoints

#### /token

- ✅ Parties MUST provide an access token via the `/token` endpoint
- ✅ Parties MUST NOT accept GET calls to the `/token` endpoint

#### POST /token

- ✅ Parties MUST support a POST call to a `/token` endpoint to create a new access token
- ✅ Parties MUST NOT pre-register clients
- ✅ Parties MUST validate that a POST request to a `/token` endpoint contains the HTTP headers as described in the table below
- ✅ Parties MUST validate that a POST request to a `/token` endpoint contains the parameters as described in the table below
- ✅ Parties MUST validate the client credentials in the `client_assertion` received in a POST to a /token endpoint, by comparing the `client_id` to the `iss` and `sub` claim in the `client_assertion` and the `subject_name` of the QSEAL used to sign the `client_assertion`
- ✅ Parties MUST include the HTTP headers as described in the table below in a response to a POST request to a `/token` endpoint
- ✅ Parties MUST include an access token as described in the table below in the HTTP payload in a response to a successful POST request to a `/token` endpoint
- ✅ Parties MUST NOT issue refresh tokens
- ✅ Parties MUST include the parameters as described in the table below in the HTTP payload in a response to a failed POST request to a `/token` endpoint

#### POST /token/revoke

- ✅ Parties MUST support a POST call to a `/token/revoke` endpoint to revoke an access token
- ✅ Parties MUST validate that a POST request to a `/token/revoke` endpoint contains the HTTP headers as described in the table below
- ✅ Parties MUST validate that a POST request to a `/token/revoke` endpoint contains the parameters as described in the table below
- ✅ Parties MUST validate the client credentials in the `client_assertion` received in a POST to a /token/revoke endpoint
- ✅ Parties MUST respond with a `200 OK` to a successful POST call to a `/token/revoke` endpoint
- ✅ Parties MUST respond with a `200 OK` to a POST call to a `/token/revoke` endpoint containing an invalid access token
- ✅ Parties MUST no longer accept the revoked the access token after a `200 OK` response is responded
- ✅ Parties MUST include the parameters as described in the table below in the HTTP payload in a response to a failed POST request to a `/token/revoke` endpoint
- ✅ Parties MAY include a `Retry-After` header in the 503 response to a `/token/revoke` endpoint to indicate the expected unavailability of the service

### /capabilities

- ✅ Parties MUST provide information about their services via the `/capabilities` endpoint

---

#### GET /capabilities

- ✅ Parties MUST support a GET call to a `/capabilities` endpoint to retrieve a list of their features (in a `capabilities_info` object).
- ✅ Parties MUST provide only `public` features to a successful GET request to the `/capabilities` endpoint, which does not include an access token
- ✅ Parties MUST validate that a GET request to the `/capabilities` endpoint includes the `Authorization` headers and contains a valid access token, when returning `restricted` features
- ✅ The trust framework catalogue MUST include a `capabilities_token` including a `capabilities_info` object in a response to a successful GET call to the `/capabilities` endpoint

---

## Data service provider endpoints

### API Service Content

- ✅ Data service providers SHOULD make use of relevant open standards in the definition of the service content of a data service

---

### Example /resources

- ✅ Data service providers MUST expose their resources in conformance with the trust framework API specifications

---

### /subscriptions

- ✅ Data service providers MUST define subscriptions for events in accordance to the `subscription` resource, when implementing a subscription
- ✅ Data service providers MUST define events for their subscriptions in accordance to the `events` resource, when implementing a subscription
- ✅ Data service providers MUST expose their subscriptions in conformance with the DSGO `/subscriptions` endpoint specifications
- ✅ Data service providers MUST determine suitable authorisation policy for their `/subscriptions` endpoint

---

#### GET /subscriptions

- ✅ Data service providers MUST support a GET call to a `/subscriptions` endpoint to retrieve a list of available subscriptions
- ✅ Data service providers MUST include a list of subscription resources available for the data service consumer in a response to a successful GET calls to the `/subscriptions` endpoint

✅ Data service providers MUST provide a count of the number of subscriptions included, in the `count` parameter, in the response to a successful GET calls to the `/subscriptions` endpoint

---

#### POST /subscriptions

✅ Data service providers MUST support a POST call to a `/subscriptions` endpoint to create a new subscription

✅ Data service providers MUST validate that the HTTP body of a POST request to a `/subscriptions` endpoint contains the following parameters, with content as defined in the `subscription` resource:

- `class`
- `start_date` (optional)
- `end_date` (optional)
- `event_type`
- `webhook_url`

✅ Data service providers MUST validate that a POST request to `/subscriptions` endpoint complies with their data service specific subscription requirements

✅ Data service providers MUST respond with a `201 Created` to a successful POST call to a `/subscriptions` endpoint

✅ Data service providers MUST include the created `subscription` resource in the HTTP body of the response to a successful POST call to the `/subscriptions` endpoint

---

#### GET /subscriptions/{id}

✅ Data service providers MUST support a GET call to a `/subscriptions/{id}` endpoint to get information about a specific subscription

✅ Data service providers MUST validate that the `{id}` of a GET request to a `/subscriptions/{id}` is valid, exists and is available to the data service consumer

✅ Data service providers MUST respond with a 200 OK to a successful GET call to a `/subscriptions/{id}` endpoint

✅ Data service providers MUST include the requested `subscription` resource in the HTTP body of the response to a successful GET call to the `/subscriptions/{id}` endpoint

✅ Data service providers MUST respond with a 404 Not found to a GET call to a `/subscriptions/{id}` endpoint when the `{id}` is not valid or available to a data service consumer

---

#### DELETE /subscriptions/{id}

✅ Data service providers MUST support a DELETE call to a `/subscriptions/{id}` endpoint to remove a specific subscription

✅ Data service providers MUST validate that the `{id}` of a DELETE request to a `/subscriptions/{id}` is valid, exists and is available to the data service consumer

- ✅ Data service providers MUST validate that the `subscription` resource being deleted complies with their data service specific subscription requirements
- ✅ Data service providers MUST respond with a 200 OK to a successful DELETE call to a `/subscriptions/{id}` endpoint
- ✅ Data service providers MUST NOT include an HTTP body in the response to a successful DELETE call to the `/subscriptions/{id}` endpoint
- ✅ Data service providers MUST set the `“status"` of `subscription/{id}` to `"inactive"` in response to a successful DELETE call to the `/subscriptions/{id}` endpoint
- ✅ Data service providers MUST respond with a 404 Not found to a DELETE call to a `/subscriptions/{id}` endpoint when the `{id}` is not a valid or available to the data service consumer

---

#### POST /subscriptions/{id}/test

- ✅ Data service providers MUST support a POST call to a `/subscriptions/{id}/test` endpoint to send a test notification to the data service consumers supplied /notifications endpoint
- ✅ Data service providers MUST validate that the HTTP body of a POST request to a `/subscriptions/{id}/test` endpoint is empty
- ✅ Data service providers MUST validate that the `{id}` of a POST request to a `/subscriptions/{id}/test` is valid, exists and is available to the data service consumer
- ✅ Data service providers MUST respond with a 202 Accepted to a successful POST call to a `/subscriptions/{id}/test` endpoint
- ✅ Data service providers MUST NOT include an HTTP body in the response to a successful POST call to the `/subscriptions/{id}/test` endpoint
- ✅ Data service providers MUST trigger the sending of a `notification` with `“eventType":“Test"` to the subscription’s webhook `url` in response to a successful POST call to the `/subscriptions/{id}/test` endpoint
- ✅ Data service providers MUST respond with a 404 Not found to a POST call to a `/subscriptions/{id}/test` endpoint when the `{id}` is not a valid or available to the data service consumer

---

### Data service consumer endpoints

#### /notifications

- ✅ Data service consumers MUST have an `/notifications` endpoint implemented before obtaining a subscription
- ✅ Data service consumers MUST support a `notification` object
- ✅ Data service consumers MUST expose their subscriptions in conformance with the DSGO `/notifications` endpoint specifications
- ✅ Data service consumers MUST determine suitable authorisation policy for their `/notifications` endpoint

---

#### POST /notifications

- ✅ Data service consumers MUST support a POST call to a `/notifications` endpoint to be able to receive notifications from data service providers
- ✅ Data service consumers MUST validate that the HTTP body of a POST request to a `/notifications` endpoint contains a valid `notification` object
- ✅ Data service consumer MUST respond with a 200 OK to a successful POST call to a `/notification` endpoint

---

### Trust framework catalogue endpoints

#### /parties

- ✅ The trust framework catalogue MUST provide information about participants via the `/parties` endpoint

---

#### GET /parties

- ✅ The trust framework catalogue MUST support a GET call to a `/parties` endpoint to retrieve a list of DSGO participants (in an array of `parties_info` objects).
- ✅ The trust framework catalogue MUST validate that the HTTP body of a GET request to the `/parties` endpoint contains the parameters as defined in the table below
- ✅ The trust framework catalogue MUST validate that the HTTP body of a GET request to the `/parties` endpoint contains at least a single parameter.
- ✅ The trust framework catalogue MUST include a `party_token` including of an (array of) `parties_info` objects in a response to a successful GET calls to the `/parties` endpoint

---

#### /trusted_list

- ✅ The trust framework catalogue MUST provide information about trusted certificate authorities via the `/trusted_list` endpoint

---

#### GET /trusted_list

- ✅ The trust framework catalogue MUST support a GET call to a `/trusted_list` endpoint to retrieve a list of DSGO participants (in an array of `trusted_list` objects).
- ✅ The trust framework catalogue MUST include a `trusted_list_token` including of an (array of) `trusted_list` objects in a response to a successful GET calls to the `/trusted_list` endpoint

---

## Identificatie

- ✅ Partijen MOETEN zich uniek identificeren wanneer ze betrokken zijn bij een datadienst

✅ Partijen MOETEN andere partijen die betrokken zijn bij een datadienst uniek identificeren

---

### Identificatie van organisaties

✅ Partijen MOETEN het EORI-nummer gebruiken als uniek identificerend kenmerk voor organisaties

✅ Partijen MOETEN het EORI-nummer gebruiken met prefix EU.EORI

---

## Autorisatie

### Autorisatiebeleid opstellen

✅ Datadienstaanbieders MOETEN het autorisatiebeleid bepalen voor elke datadienst

✅ Datadienstaanbieders MOETEN hun autorisatiebeleid vastleggen in de toegangscontroleregels van de datadienstdefinitie

---

### Autorisatie-informatie organiseren

✅ Als datadienstaanbieders gebruik maken van een access token dan MOET dit worden gedaan volgens het afsprakenstelsel

✅ Datadienstaanbieders ZOUDEN het voor de rechthebbende mogelijk MOETEN maken haar rechten over data te delegeren

✅ Als datadienstaanbieders gebruik maken van kwalificaties en eigenschappen dan MOET dit worden gedaan volgens het afsprakenstelsel

---

#### Access token

✅ Als partijen gebruik willen maken van een access token dan, MOETEN ze deze beschikbaar stellen via een /token endpoint

✅ Partijen MOETEN verifiëren dat het certificaat waarmee de Basis JWT is getekend uitgegeven en ondertekend is door een certificaatautoriteit op de vertrouwde lijst van DSGO

✅ Partijen MOETEN verifiëren dat het certificaat waarmee Basis JWT is getekend valide is

✅ Partijen MOETEN bij elk verzoek om een access token, de identiteit van de aanvrager authenticeren door de identiteit uit het certificaat te vergelijken met die uit het access token verzoek. Indien deze niet matchen met elkaar, MOETEN het verzoek worden afgewezen.

✅ Partijen MOETEN bij een access token verzoek de status van een partij binnen het DSGO verifiëren bij de stelselcatalogus

---

#### Delegaties

✅

Als gedelegeerde datadienstgebruikers een datadienst kunnen afnemen MOETEN datadienstaanbieders vaststellen waar delegaties geregistreerd mogen worden

✅ Als de rechthebbende gebruik wil maken van de mogelijkheid om haar rechten te delegeren dan MOET de rechthebbende binnen de opties aangeboden in een datadienst bepalen waar haar delegaties geregistreerd worden

✅ Als een datadienstaanbieder de mogelijkheid biedt voor de rechthebbende om zelf haar delegaties te beheren dan MOET dit worden gedaan volgens het afsprakenstelsel

✅ Als een datadienstaanbieder de mogelijkheid biedt voor rechthebbende om haar delegaties te registreren bij de datadienstaanbieder dan MOET de datadienstaanbieder dit mogelijk maken voor de rechthebbende

✅ Als een datadienstaanbieder de mogelijkheid biedt voor rechthebbende om haar delegaties te registreren bij een autorisatieregister dan MOET dit worden gedaan volgens het afsprakenstelsel

---

### Autorisatiebesluit nemen

✅ Datadienstaanbieders ZOUDEN MOETEN handelen naar haar autorisatiebeleid

---

## Informatiebeveiliging

✅ Partijen ZOUDEN een risicoanalyse uit MOETEN voeren

✅ Partijen ZOUDEN passende informatiebeveiligingsmaatregelen MOETEN nemen

✅ Partijen ZOUDEN andere partijen waarmee wordt samengewerkt MOETEN aansporen passende informatiebeveiligingsmaatregelen te nemen

---

### Transport Layer Security

✅ Partijen MOETEN API endpoints beveiligen met minimaal TLS v1.2

✅ Partijen ZOUDEN API endpoints MOETEN beveiligen met TLS v1.3

✅ Partijen MOETEN API verzoeken die niet beveiligd zijn met TLS v1.2 of TLS v1.3 afwijzen

✅ Partijen MOETEN voor alle machine-to-machine interacties gebruik maken van one-way (server only) TLS

✅ Partijen MOETEN voor alle human-to-machine interacties gebruik maken van one-way (server only) TLS

✅ Partijen MOETEN bij toepassing van het TLS protocol certificaten gebruiken met een minimale sleutellengte van 2048 bits en maximale geldigheid van twee jaar

✅ Partijen MOETEN QWACS als certificaat gebruiken voor het one-way (server only) TLS protocol

✅ Partijen MOETEN alle root certificaten voor QWACs van CAs op de EU/EEA List of Trusted Lists (LOTL) en PKIO accepteren

---

### JSON Web Tokens (JWT)

✅ Partijen MOETEN alle JWTs ondertekenen als een JSON Web Signature (JWS) zoals beschreven in RFC 7515

✅ Partijen MOETEN alle getekende Geavanceerde JWTs formatteren volgens JWS Compact Serialisation

✅ Partijen MOETEN het RS256 algoritme gebruiken bij het ondertekenen van alle JWTs

✅ Partijen MOETEN in Basis JWTs de parameters gebruiken  als JWT headers zoals opgesteld in de onderstaande tabel

✅ Partijen MOETEN in Geavanceerde JWTs de parameters gebruiken als JWT headers zoals opgesteld in de onderstaande tabel

✅ Partijen MOGEN in alle JWTs andere parameters NIET als JWT headers gebruiken

✅ Partijen MOETEN in alle Basis JWTs de JWT claims opstellen volgens het “JWT Bearer profile” als beschreven in RFC 7523 zoals opgesteld in de onderstaande tabel

✅ Partijen ZOUDEN in alle Basis JWTs NIET andere JWT claims MOETEN definiëren en gebruiken, afhankelijk van het specifieke gebruik van de JWT

✅ Partijen MOETEN in alle Basis JWTs alle JWT claims binnen 30 seconden laten verlopen, aantoonbaar door de combinatie van `iat` en `exp` claims.

✅ Partijen MOETEN in alle Basis JWTs de JWT claims de `iat` en `exp` claims noteren in seconden en MOGEN `iat` en `exp` claims NIET noteren in milliseconden

✅ Partijen MOETEN in alle Geavanceerde JWTs de JWT payload “detached“ maken van de handtekening, zoals beschreven in RFC 7515 Appendix F

✅ Partijen MOETEN in alle Geavanceerde JWTs de JWT claims opstellen volgens de parameters zoals beschreven in `"sigD"` van de JWT Header.

✅ Partijen ZOUDEN in alle Geavanceerde JWTs NIET andere JWT claims MOETEN definiëren en gebruiken, afhankelijk van het specifieke gebruik van de JWT

✅ Partijen MOETEN een getekende JWT maar één keer accepteren

✅ Partijen MOETEN een JWT niet accepteren als:

- De handtekening ongeldig is,
- Deze niet aan hen geadresseerd is, op basis van de `aud` claim,
- Deze niet verlopen is, op basis van de `exp` claim,
- Deze niet eerder ontvangen is, op basis van de `jti` claim met inachtneming van de verlooptijd,
- De geclaimde ondertekeningstijd, op basis van de `sigT` claim, niet valt binnen redelijke verwachte tijdvenster voor transacties vergeleken met de lokaal beheerde tijd

✅ Partijen MOGEN gebruik maken van JWE als beschreven in RFC 7516

---

### Ondertekening

✅ Partijen MOETEN alle QSEALS gebruiken voor het tekenen van JWTs

✅ Partijen MOETEN alle root certificaten voor QSEALs van CAs op de EU/EEA List of Trusted Lists (LOTL) en PKIO accepteren

---

### Onweerlegbaarheid

✅ Als partijen willen dat een verzoek of respons onweerlegbaar is, MOETEN ze de `"Digest"` HTTP Header toevoegen in berichten zoals beschreven in de tabel hieronder.

✅ Als partijen willen dat een bericht onweerlegbaar is, MOETEN ze een Geavanceerde JWT toevoegen in het bericht

✅ Als datadienstaanbieders willen dat elke datadienstverzoek onweerlegbaar is, MOETEN ze dit vastleggen in de datadienstdefinitie

✅ Als datadienstaanbieders onweerlegbare datadienstresponsen aanbied, MOETEN ze dit vastleggen in de datadienstdefinitie

---

## Service level agreements

### SLAs voor datadienstaanbieders

✅ Datadienstaanbieders MOETEN het openstellingsvenster van de datadienst definiëren en beschikbaar stellen aan datadienstgebruikers

✅ Datadienstaanbieders MOETEN het onderhoudsvenster van de datadienst definiëren en beschikbaar stellen aan datadienstgebruikers

✅ Datadienstaanbieders MOETEN het onderhoudsvenster plannen buiten reguliere kantooruren

✅ Datadienstaanbieders MOGEN gepland onderhoud uitvoeren op elke tijdstip, als er geen uitval wordt verwacht

✅ Datadienstaanbieders ZOUDEN datadiensten binnen het beschikbaarheidsvenster minimaal 95% van de tijd beschikbaar MOETEN stellen aan datadienstgebruikers

✅ Datadienstaanbieders ZOUDEN op 95% van API verzoeken binnen 2 seconden MOETEN reageren binnen het beschikbaarheidsvenster

✅ Datadienstaanbieders ZOUDEN op 99% van API verzoeken binnen 5 seconden MOETEN reageren binnen het beschikbaarheidsvenster

✅ Datadienstaanbieders ZOUDEN ten minste 100 API verzoeken MOETEN kunnen verwerken binnen het beschikbaarheidsvenster

✅ Datadienstaanbieders ZOUDEN op een passende frequentie een back-up MOETEN maken van data belangrijk voor de datadienst

- ✅ Datadienstaanbieders ZOUDEN de back-ups MOETEN opslaan voor een passende periode
- ✅ Datadienstaanbieders ZOUDEN bereikbaar MOETEN zijn voor ondersteuning via e-mail
- ✅ Datadienstaanbieders ZOUDEN binnen een werkdag na ontvangst van een vraag, verzoek of klacht MOETEN aangeven dat hiervan kennis is genomen
- ✅ Datadienstaanbieders ZOUDEN binnen vijf werkdagen na ontvangst van een vraag, verzoek of klacht deze MOETEN beantwoorden of oplossen
- ✅ Datadienstaanbieders MOETEN aan alle releasebeheer eisen voldoen

---

## Operationele processen

### Toezicht en handhaving

#### Incidentbeheer

- ✅ De beheerorganisatie MOET een incidentcoördinator aanwijzen na een melding van een incident
- ✅ Partijen MOETEN incidenten direct na ontdekking melden bij de beheerorganisatie
- ✅ Partijen ZOUDEN voor alle Prioriteit 1 en Prioriteit 2 incidenten waarbij zij betrokken zijn een incidentmanager 24u per dag, 7 dagen per week beschikbaar MOETEN stellen
- ✅ Partijen MOETEN voor alle Prioriteit 1 en Prioriteit 2 incidenten waarbij zij betrokken zijn een incidentmanager beschikbaar stellen
- ✅ De incidentcoördinator MOET het incidentbeheer proces na de melding van een incident coördineren.
- ✅ De incidentcoördinator MOET kunnen optreden als een neutrale partij bij het incident
- ✅ De incidentmanager MOET voor een Prioriteit 1 incident een update delen met de incidentcoördinator binnen 2 uur van elke belangrijke update en elke 4 uur bij geen update
- ✅ De incidentmanager MOET voor een Prioriteit 2 incident een update delen met de incidentcoördinator binnen 2 uur van elke belangrijke update aan het einde van elke werkdag bij geen update
- ✅ De incidentmanager MOET voor een Prioriteit 3 incident een volledige update delen met de incidentcoördinator aan het einde van elke werkdag

---

#### Classificatie incidenten

- ✅ Partijen die een incident melden MOETEN de naam van de verondersteld veroorzakende partij met een onderbouwing van de constatering/vermoeden, datum, tijd, ingeschatte incident classificatie en impact op de datadienst melden bij de rapportage over een incident

- ✅ De incidentcoördinator MOET het incident beoordelen en legt het classificatie niveau vast

### Handhaving

- ✅ De beheerorganisatie MOET voordat het overgaat tot handhaven de belangen van het DSGO, de betrokken partijen en de deelnemers in overweging nemen en het doel van de maatregel afwegen tegen de gevolgen
- ✅ De beheerorganisatie MAG een handhavende maatregel (waarschuwing, schorsing of uitsluiting) opleggen bij een overtreding om de vertrouwelijkheid en/of integriteit van het DSGO afsprakenstelsel te beschermen
- ✅ Partijen MOETEN te allen tijde handelen in overeenstemming met het afsprakenstelsel

#### Classificatie overtredingen

- ✅ De beheerorganisatie MOET de overtreding beoordelen en legt het classificatie niveau vast

### Change en release management

- ✅ De beheerorganisatie MOET het change en release management proces begeleiden
- ✅ De beheerorganisatie MAG een Request For Change (RFC) indienen conform het change en release management proces
- ✅ De change advisory board MOET de beheerorganisatie adviseren in de behandeling van Requests For Change (RFCs)
- ✅ Deelnemers MOGEN een Request For Change (RFC) indienen conform het change en release management proces
- ✅ Partijen MOGEN een Request For Change (RFC) indienen conform het change en release management proces
- ✅ De beheerorganisatie MAG in het geval van spoed besluiten om af te wijken van het standaard change en release proces
- ✅ De beheerorganisatie MAG in het geval van een kleine wijziging, die geen impact heeft op de technische werking of juridische basis, deze uitvoeren zonder het standaard change en release proces te doorlopen

#### Versie richtlijnen

- ✅ De beheerorganisatie MOET bij een release van het afsprakenstelsel de wijziging van versienummer bepalen
- ✅ De beheerorganisatie MOET releases communiceren middels de versie richtlijnen

## Marktvoorzieningen

- ✅ Authenticatiediensten MOETEN voldoen aan alle eisen van een Identity Provider volgens iSHARE

✅ Autorisatieregisters MOETEN voldoen aan alle eisen van een Autorization Registry volgens iSHARE

---

# Specifieke afspraken

## BIM in datadiensten

✅ Als datadiensten gebruik maken van gestructureerde geometrische modellen (een BIM-model) dan MOETEN partijen alle `DSGO.BIM` afspraken volgen

✅ `DSGO.BIM`: Datadienstaanbieders ZOUDEN IFC4 ADD2 TC1 (v4.0.2.1) MOETEN ondersteunen

✅ `DSGO.BIM`: Datadienstaanbieders ZOUDEN aanlevereisen aan een IFC4 model MOETEN specificeren met IDS v0.9.6 indien IDS het technisch toe laat

---

### BIM voor vergunning of melding afhandelen

✅ Als datadiensten gebruikt worden in de Fase 01.02 Vergunning of Melding Afhandelen, en gebruik maken van gestructureerde geometrische modellen (een BIM-model) dan MOETEN partijen alle `DSGO.BIM.Vergunning` afspraken volgen

✅ `DSGO.BIM.Vergunning`: Datadienstaanbieders MOETEN IFC4 ADD2 TC1 (v4.0.2.1) ondersteunen

✅ `DSGO.BIM.Vergunning`: Datadienstaanbieders MOETEN aanlevereisen met IDS v0.9.6 beschrijven indien IDS het technisch toe laat

---

#### BIM voor vergunning of melding afhandelen voor gebouwen met een woonfunctie

✅ Als datadiensten gebruikt worden in de Fase 01.02 Vergunning of Melding Afhandelen, en gebruik maken van gestructureerde geometrische modellen (een BIM-model) voor een gebouw met een woonfunctie dan MOETEN partijen alle `DSGO.BIM.Vergunning.Woonfunctie` afspraken volgen

✅ `DSGO.BIM.Vergunning.Woonfunctie`: Datadienstaanbieders MOETEN ondersteunen dat het lokale nulpunt een verwijzing bevat naar het Rijksdriehoeksstelsel ( `RD_new` ) en de hoogte t.o.v. NAP, door bij `IFCClass:IfcProjectedCRS` de waarde `Name:EPSG:7415` te gebruiken of `Name:EPSG:28992` en als Z-waarde de hoogte tegenover NAP te gebruiken

✅ `DSGO.BIM.Vergunning.Woonfunctie`: Datadienstaanbieders MOETEN ondersteunen dat het BIM-model de `IFCClass:IFCMAPCONVERSION` bevat met attributen `Eastings`, `Northings` en `OrthogonalHeight` ingevuld

✅ `DSGO.BIM.Vergunning.Woonfunctie`: Datadienstaanbieders MOETEN ondersteunen dat de bouwlagen gedefinieerd worden met `IFCClass:IFCBUILDINGSTOREY` en `attribuut Name` volgens de bouwlaagnaamgevingsmethode van de BIM basis ILS v2

✅ `DSGO.BIM.Vergunning.Woonfunctie`: Datadienstaanbieders MOETEN ondersteunen dat elk geometrisch object (bv. `IfcSpace` ) een relatie heeft met een bouwlaag via `IFCRELAGGREGATES` met een element uit `IFCClass:IFCBUILDINGSTOREY`

✅

`DSGO.BIM.Vergunning.Woonfunctie`: Datadienstaanbieders MOETEN ondersteunen dat het BIM-model de NEN2580 normen voor oppervlakken (BVO/GO) en ruimte (NVO) bevat

✅ `DSGO.BIM.Vergunning.Woonfunctie`: Datadienstaanbieders MOETEN ondersteunen dat het brutovloeroppervlak (BVO) beschreven wordt als `IFCClass:IfcSpatialZone` met predefined type `USERDEFINED` met attributen uit onderstaande tabel

✅ `DSGO.BIM.Vergunning.Woonfunctie`: Datadienstaanbieders MOETEN ondersteunen dat het gebruiksoppervlak (GO) beschreven wordt als `IFCClass:IfcSpatialZone` met predefined type `USERDEFINED` met attributen uit onderstaande tabel

✅ `DSGO.BIM.Vergunning.Woonfunctie`: Datadienstaanbieders MOETEN ondersteunen dat het nettovloeroppervlak (NVO) beschreven wordt als `IFCClass:IfcSpace` met onderstaande tabel

✅ `DSGO.BIM.Vergunning.Woonfunctie`: Datadienstaanbieders MOETEN ondersteunen dat ruimten ( `IfcSpaces` ) die bij dezelfde wooneenheid horen, gegroepeerd worden met een `IFCClass:IfcZone` met attributen uit onderstaande tabel

# Begrippenlijst (glossary)

Alle begrippen zijn in het Nederlands (links) en Engels (rechts) gedefineerd, wanneer begrippen gebruikmaken van dezelfde term, worden deze niet herhaald in de koptekst. Bij het opstellen van deze begrippenlijst is zoveel mogelijk gebruik gemaakt van bestaande begrippen die waar nodig zijn aangepast naar de DSGO context.

> Merk op, deze pagina geeft enkel definities van begrippen. Voor meer informatie over de context van de termen wordt verwezen naar het eerste gebruik van de term in het afsprakenstelsel.

**English:** All glossary terms are defined in Dutch (left) and English (right). if the Dutch and English terms are identical, it is not repeated in the header. During the creation of this glossary, existing definitions were re-used where possible. In case needed, these definitions were adjusted to the context of DSGO.

> Note, this page provides definitions of terms only. For more information on the context of the terms, please refer to the first use of the term in the Trust Framework.

- Ecosysteem (Ecosystem)
- EORI
- Federatief ecosysteem (Federated ecosystem)
- Gebruiksvoorwaarden (Terms of use)
- Gebeurtenis (Event)
- Human-to-machine
- Identificatie (Identification)
- Identificatiedienst (Identity Provider)
- Identificerend kenmerk (Identifier)
- Incident (Incident)
- Incidentcoördinator (Incident coordinator)
- Inlogmiddel (login)
- Interoperabiliteit (Interoperability)
- Licenties (License)
- Machine-to-machine
- Marktvoorzieningen (Market facilities)
- Notificatie (Notification)
- Overtreding (Violation)
- Onweerlegbaarheid (Non-repudiation)
- Rechthebbende (Entitled party)
- Resource
- Richtinggevende principes (Guiding principles)
- SLAs
- Sleutelrol (Key role)
- Stelselcatalogus (Trust framework catalogue)
- Stelselvoorzieningen (Trust framework facilities)
- Voorzieningen (Facilities)

---

### Abonnement (Subscription)

Een overeenkomst tussen een datadienstaanbieder en een datadienstgebruiker om notificaties te ontvangen bij specifieke gebeurtenissen gerelateerd aan een datadienst.

An agreement between a data service provider and a data service consumer to receive notifications on specific events related to a data service.

**Gebaseerd op (Based on):** nvt (n/a)

---

### Access token

Een ‘string’ met een specifiek toepassingsgebied, levensduur en andere toegangsvoorwaarden die de autorisatie (namens de rechthebbende) van een specifieke toepassing vertegenwoordigt.

A string denoting a specific scope, lifetime, and other access attributes which represents the Authorization (on behalf of the entitled party) of a specific application.

**Gebaseerd op (Based on):** OAuth 2.0

---

### Afsprakenstelsel (Trust framework)

Afsprakenstelsels zijn nauwe samenwerkingsvormen van verschillende partijen uit het bedrijfsleven, de overheid en de wetenschap, die producten of diensten leveren, op basis van vastgelegde eisen.

**Gebaseerd op (Based on):** Logius

Trust frameworks are close collaborations of different parties from industry, government and science, which provide products or services, based on defined requirements.

---

### Afsprakenstelsel DSGO (DSGO trust framework)

Het afsprakenstelsel DSGO is een set afspraken tussen deelnemers aan het DSGO en is het fundament voor harmonisatie en vertrouwen om een federatief ecosysteem voor data delen te realiseren.

**Gebaseerd op (Based on):** nvt (n/a)

The DSGO trust framework is a set of unified agreements between participants of the DSGO and facilitates harmonisation and trust to realise a federated ecosystem for data sharing.

---

### Application programming interface

Een application programming interface (API) is een gestructureerd en gedocumenteerd koppelvlak voor communicatie tussen applicaties.

**Gebaseerd op (Based on):** Geonovum Nederlandse API Strategie

An application programming interface (API) is a structured and documented interface for communication between applications.

---

### Authenticatie (Authentication)

Het proces waarmee de geldigheid van een geclaimde identiteit van een partij wordt geverifieerd

**Gebaseerd op (Based on):** Data Sharing Coalition

The process where the validity of a partij claiming an identity is verified.

---

### Authenticatiedienst (Authentication service)

Een partij die diensten biedt voor het creëren, onderhouden, beheren en valideren van identiteiten van natuurlijke personen (mensen) tijdens het gebruik van datadiensten en/of het registreren van autorisaties in het DSGO

**Gebaseerd op (Based on):** iSHARE

A party that offers services to create, maintain, manage and validate identities form natural persons (people)while using data services and/or registering authorizations in the DSGO

---

### Autorisatie (Authorization)

Het hebben van rechten of toestemming en het proces waarbij een partij rechten of toestemming krijgt om een specifieke actie uit te voeren.

**Gebaseerd op (Based on):** nvt (n/a)

Having rights or permission and the process by which a party obtains rights or permission to perform a specific action.

### Autorisatiebeleid (Authorization policy)

Per datadienst wordt autorisatiebeleid vastgelegd wat de logica en voorwaarden beschrijft waaraan moet worden voldaan om specifieke rechten te verkrijgen in de context van de dienst.

**Gebaseerd op (Based on):** nvt (n/a)

Per data service the authorization policy defines the logic and conditions which must be met to obtain specific rights in the context of the service.

### Autorisatiebesluit (Authorization decision)

Het autorisatiebesluit is het proces waarbij een datadienst verzoek wordt gecontroleerd of deze voldoet aan de gestelde eisen van het autorisatiebeleid.

**Gebaseerd op (Based on):** nvt (n/a)

The authorisation decision is the process whereby a data service request is validated against the requirements of the of the authorisation policy.

### Autorisatie-informatie (Authorization information)

De informatie die wordt opgehaald en getoetst tegen het autorisatiebeleid om een autorisatiebesluit te nemen

**Gebaseerd op (Based on):** nvt (n/a)

The information retrieved and tested against the authorization policy to make an authorization decision

### Autorisatieregister (Authorization register)

De Partij die diensten biedt voor het registeren, beheren en ontsluiten van delegaties van rechthebbenden aan derden, zodat derden toegang kunnen krijgen tot een datadienst.

**Gebaseerd op (Based on):** iSHARE

The party that offer services for registering, managing and disclosing delegations from entitled parties to third parties so that third parties can access a data service.

### Beheerorganisatie DSGO (DSGO trust framework authority)

De beheerorganisatie DSGO is verantwoordelijk het (laten) uitvoeren van de activiteiten rondom beheer, adoptie en doorontwikkeling van het DSGO.

**Gebaseerd op (Based on):** nvt (n/a)

The DSGO trust framework authority is responsible for executing activities regarding management, adoption and continuous development of the DSGO or letting those activities be executed by a third party

### Betrouwbaarheidsniveaus (Level of assurance)

De mate waarin een geclaimde identiteit gegarandeerd kan worden.

**Gebaseerd op (Based on):** iSHARE

The degree of confidence in the claimed identity of a person.

### Conformiteitstest-tool (Conformance test-tool)

Een software hulpmiddel om te verifiëren of datadiensten voldoen aan de generieke afspraken zoals opgesteld in het afsprakenstelsel DSGO

A software tool to verify that data services comply with the generic agreements as established in the DSGO trust framework

**Gebaseerd op (Based on):** nvt (n/a)

---

### Data

Een herinterpreteerbare digitale weergave van ruwe gegevens, informatie of documenten, geschikt voor communicatie, interpretatie of verwerking.

A reinterpretable digital representation of raw data, information or documents, suitable for communication, interpretation, or processing.

**Gebaseerd op (Based on):** Data Sharing Coalition

---

### Datadienstbroker (Data service broker)

Een partij die bij uitvoering van een datadienst optreedt als (technisch) dienstverlener namens een datadienstaanbieder en/of datadienstgebruiker

A party acting as a (technical) service provider on behalf of a data service provider and/or data service consumer while executing a data service

**Gebaseerd op (Based on):** nvt (n/a)

---

### Datadienst (Data service)

Een dienst aangeboden door een datadienstaanbieder met als doel om data te delen en/of het bewerken van data.

Any service offered by a data service provider aimed at sharing and/or processing data.

**Gebaseerd op (Based on):** Data Sharing Coalition

---

### Datadienstaanbieder (Data service provider)

De partij die verantwoordelijk is voor het definiëren van één of meer datadiensten en deze aan te bieden en leveren conform haar datadienstdefinitie

The party that is responsible for defining one or more data services and to offer and deliver those in accordance with their data service definition

**Gebaseerd op (Based on):** nvt (n/a)

---

### Datadienstgebruiker (Data service consumer)

De partij die verantwoordelijk is voor het afnemen van een datadienst, voor het voldoen aan de voorwaarden, verplichtingen en mogelijke delegatie voorwaarden van de datadienst conform de datadienstdefinitie

The party that is responsible for using a data service, complying with the requirements, obligations and possible delegation requirements of the data service accordance with the data service definition

**Gebaseerd op (Based on):** nvt (n/a)

---

### Datadienst ondekking (Data service discovery)

Het mechanisme waarmee een datadienstgebruiker een datadienst en haar datadienstaanbieder kan vinden gebruikmakend van een stelselcatalogus.

**Gebaseerd op (Based on):** Data Sharing Coalition

The mechanism through which a data service consumer can find a data service and its data service provider by making use of the trust framework catalogue.

---

### Data delen (Data sharing)

De machinaal verwerkbare uitwisseling van computer leesbare en/of menselijk leesbare gestructureerde data via een datadienst tussen een datadienstaanbieder en datadienstgebruiker.

**Gebaseerd op (Based on):** Data Sharing Coalition

The machine actionable exchange of machine readable and/or human readable structured data through a data service between a data service provider and a data service consumer.

---

### Deelnameovereenkomst (Participation agreement)

De deelnameovereenkomst verklaart het afsprakenstelsel DSGO van toepassing waarmee het onlosmakelijk verbonden is met het afsprakenstelsel. Met het tekenen van de deelnameovereenkomst wordt een partij deelnemer aan het DSGO.

**Gebaseerd op (Based on):** nvt (n/a)

The participation agreement declares the DSGO trust framework applicable with which it is inseparable from the trust framework. By signing the participation agreement, a party becomes a participant in the DSGO.

---

### Deelnemer (Participant)

Deelnemers (aan het DSGO) zijn partijen die succesvol zijn toegetreden tot het DSGO en een deelnameovereenkomst hebben gesloten met de beheerorganisatie en zich daarmee commiteren aan het afsprakenstelsel.

**Gebaseerd op (Based on):** Data Sharing Coalition

(DSGO) participants are parties who have succesfully joined the DSGO and have signed a participation agreement with the trust framework authority and thus commit to the trust framework.

---

### Delegatie (Delegation)

Het overdragen van een bevoegdheid aan een ander dat de bevoegdheid gaat uitoefenen.

**Gebaseerd op (Based on):** nvt (n/a)

Transferring a power to another person who will exercise the power.

---

### Developer portal

Een online interface wat ontwikkelaars ondersteunt bij implementatie van datadiensten op basis van het afsprakenstelsel DSGO

Gebaseerd op (Based on): nvt (n/a)

An online interface that supports developers in implementing data services based on the DSGO trust framework

---

### DSGO

Het DSGO faciliteert een netwerk van datadiensten om in de gebouwde omgeving data te delen en/of te bewerken in een federatief ecosysteem o.b.v. het afsprakenstelsel en voorzieningen.

**Gebaseerd op (Based on):** nvt (n/a)

The DSGO facilitates a network of data services to to share and/or process data in the built environment within a federated ecosystem based on a trust framework and facilities.

---

### DSGO-programma (DSGO-programme)

Het Digitaal Stelsel Gebouwde Omgeving (DSGO) programma loopt tot mid 2024 met als doel het ontwerpen, realiseren en in beheer (doen) nemen van het DSGO.

**Gebaseerd op (Based on):** nvt (n/a)

The 'Digitaal Stelsel Gebouwde Omgeving' (DSGO) programme runs until mid 2024 with the goal of designing, implementing and take (or have taken) into management of the DSGO.

---

### Ecosysteem (Ecosystem)

een gedistribueerd, aanpassend, open systeem die eigenschappen toont van zelforganisatie, schaalbaarheid en duurzaamheid.

**Gebaseerd op (Based on):** nvt (n/a)

a distributed, adaptive, open system with properties of self-organisation, scalability and sustainability.

---

### EORI

Een Europees identificatienummer dat binnen de EU wordt gebruikt om partijen op uniforme wijze te identificeren.

**Gebaseerd op (Based on):** Belastingdienst

An European identification number that is used to identify parties in a uniform manner with the EU.

---

### Federatief ecosysteem (Federated ecosystem)

Een ecosysteem waar partijen in verschillende rollen samenwerken en op elkaar vertrouwen terwijl ze hun eigen zelfstandigheid houden.

**Gebaseerd op (Based on):** nvt (n/a)

An ecosystem where parties in various roles cooperate and trust each other while maintaining their own independence.

---

### Gebruiksvoorwaarden (Terms of use)

De voorwaarden waaraan datadienstgebruikers en rechthebbenden zich moet houden ten aanzien van het gebruik van datadiensten en data in het DSGO.

**Gebaseerd op (Based on):** nvt (n/a)

The terms of use to which data service consumers and entitled parties must adhere regarding the use of data services and data in the DSGO.

---

### Gebeurtenis (Event)

Een (door de datadienstaanbieder) gedefinieerde specifieke wijziging in de bronsystemen van een datadienstaanbieder. Bijvoorbeeld het wijzigen van de brondata.

**Gebaseerd op (Based on):** nvt (n/a)

A specific change (defined by the data service provider) to a data service provider's source systems. For example, changing the source data.

---

### Human-to-machine

Een human-to-machine interactie is een interactie waarbij een persoon met een machine communiceerd middels een user-interface.

**Gebaseerd op (Based on):** nvt (n/a)

A human-to-machine interaction is one in which a person communicates with a machine through a user-interface.

---

### Identificatie (Identification)

het proces waarbij een identiteit wordt aangeduid aan of wordt geclaimd door een partij die een rol vervuld in het afsprakenstelsel.

**Gebaseerd op (Based on):** iSHARE

The process by which an identity is designated to or is claimed by a party furfilling a role within the trust framework.

---

### Identificatiedienst (Identity Provider)

Zie Authenticatiedienst

**Gebaseerd op (Based on):** iSHARE

see Authentication service

---

### Identificerend kenmerk (Identifier)

Een uitdrukking van een identiteit.

**Gebaseerd op (Based on):** nvt (n/a)

An expression of an identity.

---

### Incident (Incident)

Een incident is een ongewenste gebeurtenis die niet direct oplosbaar is en:

- niet tot de standaardoperatie van het DSGO of de beschikbare datadiensten behoort, en/of
- mogelijk leidt tot het verlies van vertrouwen, veiligheid en integriteit van het afsprakenstelsel en/of daarop geïmplementeerde datadiensten.

**Gebaseerd op (Based on):** nvt (n/a)

An incident is an undesired event that is not immediately solvable and:

- is not part of the standard operation of the DSGO or available data services and/or
- potentially results in the loss of trust, security and integrity of the trust framework and/or data services implemented on it.

---

### Incidentcoördinator (Incident coordinator)

De incidentcoördinator is een neutrale partij verantwoordelijk voor het coördineren van het incidentbeheer proces.

**Gebaseerd op (Based on):** nvt (n/a)

The incident coordinator is a neutral party responsible for coordinating the incident management proces.

---

### Inlogmiddel (login)

Nader nog uit te werken

**Gebaseerd op (Based on):** nvt (n/a)

To be determined

---

### Interoperabiliteit (Interoperability)

De mogelijkheid van partijen om te interacteren om wederzijds voordelige doelen, waarbij informatie en kennis tussen deze partijen worden uitgewisseld via de bedrijfsprocessen die zij ondersteunen, door middel van de uitwisseling van data tussen hun ICT-systemen.

**Gebaseerd op (Based on):** New European Interoperability Framework

The ability of organisations to
interact towards mutually beneficial goals, involving the sharing of information
and knowledge between these organisations, through the business processes
they support, by means of the exchange of data between their ICT systems.

---

### Licenties (License)

De gebruiksrechten die de datadienstgebruiker als beperkt recht verkrijgt om data van een datadienstaanbieder (met toestemming van de rechthebbende) te delen en/of te bewerken.

**Gebaseerd op (Based on):** nvt. (n/a)

The rights of use that the data service consumer obtains as a limited right to share and/or edit data from a data service provider (with permission from the entitled party).

---

### Machine-to-machine

Een machine-to-machine interactie is een interactie tussen twee machines zonder tussenkomst van een persoon.

**Gebaseerd op (Based on):** nvt (n/a)

A machine-to-machine interaction is an interaction between two machines without the intervention of a person.

---

### Marktvoorzieningen (Market facilities)

Voorzieningen die geleverd worden door marktpartijen in de gebouwde omgeving

**Gebaseerd op (Based on):** nvt (n/a)

Facilities which are provided by the market parties in the built environment

---

### Notificatie (Notification)

Een melding van een event van de datadienstaanbieder, ontvangen door de datadienstgebruiker onder de voorwaarden van een abonnement.

**Gebaseerd op (Based on):** nvt (n/a)

A notification of an event from the data service provider, received by the data service consumer under the condition of a subscription.

---

### Overtreding (Violation)

Een overtreding is een incident dat wordt veroorzaakt doordat een deelnemer zich niet aan de in het DSGO afsprakenstelsel opgestelde afspraken houdt

**Gebaseerd op (Based on):** nvt (n/a)

A violation is an incident caused by a participant's failure to comply with the agreements set out in the DSGO trust framework.

---

### Onweerlegbaarheid (Non-repudiation)

De borging dat een bewerking of gebeurtenis niet nu noch later ontkend kan worden door de betrokken partijen.

**Gebaseerd op (Based on):** nvt (n/a)

The assurance that an operation or event cannot be denied now or later by the parties involved.

---

### Rechthebbende (Entitled party)

De entiteit die gebruiksrechten heeft over data en zeggenschap heeft over het gebruikersrecht van derde partijen betreffende die data

**Gebaseerd op (Based on):** nvt (n/a)

The entity that holds user rights over data and can transfer user rights regarding that data to third parties

---

### Resource

Een resource is een object met een type, bijbehorende data, relaties met andere resources en een aantal operaties om deze te bewerken.

**Gebaseerd op (Based on):** Geonovum Nederlandse API Strategie

A resource is an object with a type, associated data, relationships to other resources and operations to manipulate it.

---

### Richtinggevende principes (Guiding principles)

Principes die richting geven aan besluiten over afspraken gedurende het vaststellen en onderhouden van het afsprakenstelsel.

**Gebaseerd op (Based on):** Data Sharing Coalition

Principles that give direction in the decision-making process of establishing and maintaining the trust framework.

---

### SLAs

Serviceniveau-overeenkomsten (of dienstenniveau-overeenkomsten) zijn afspraken over de kwaliteit, beschikbaarheid en verantwoordelijkheden van datadiensten.

**Gebaseerd op (Based on):** nvt (n/a)

Service Level Agreements are agreements on the quality, availability and responsibilities of data services.

---

### Sleutelrol (Key role)

Sleutelrollen zijn direct betrokken bij elke datadienst en zijn essentieel voor het functioneren van het DSGO. Het DSGO kent drie sleutelrollen, de datadienstaanbieder, datadienstgebruiker en rechthebbende.

**Gebaseerd op (Based on):** nvt (n/a)

Key roles are directly involved in any data service and are essential to the functioning of the DSGO. The DSGO has three key roles, the data service provider, data service consumer and the entitled party.

---

### Stelselcatalogus (Trust framework catalogue)

Catalogus die alle nodige informatie bevat om datadiensten, deelnemers, en voorzieningen te vinden, begrijpen en gebruiken.

**Gebaseerd op (Based on):** nvt (n/a)

Catalogue that contains all necessary information to find, understand, and make use of data services, participants, and facilities.

---

### Stelselvoorzieningen (Trust framework facilities)

Voorzieningen die geleverd worden door de beheerorganisatie van het DSGO.

**Gebaseerd op (Based on):** nvt (n/a)

Facilities which are provided by the DSGO trust framework authority.

---

### Voorzieningen (Facilities)

Componenten die ondersteunende functionaliteiten bieden die nodig zijn voor het functioneren van het DSGO. Zoals bijvoorbeeld een autorisatieregister, authenticatiedienst en de stelselcatalogus.

**Gebaseerd op (Based on):** nvt (n/a)

Components that provide supporting functionalities necessary for the operation of the DSGO. For example, an authorization register, authentication service and the scheme catalogue.

# FAQ

Deze sectie bevat een overzicht van enkele veel gestelde vragen met antwoorden:

richtinggevende principes van het DSGO. De input wordt vervolgens gestructureerd in onderwerpen die ter discussie kunnen worden gesteld in werkgroepen. De resultaten van de werkgroepen worden opgenomen in het afsprakenstelsel als concept afspraken en worden behandeld in de volgende iteratie van een publieke review. Op deze wijze kan de hele sector via de publieke review input leveren op de concept afspraken. Indien de publieke review daarvoor aanleiding geeft, kan een concept afspraak opnieuw als input worden ingediend.

Voor meer informatie zie deze pagina:

Aanpak ontwikkeling van het Afsprakenstelsel DSGO

Hoe worden specifieke afspraken in het afsprakenstelsel DSGO ontwikkeld?

Vergelijkbaar met generieke afspraken komen specifieke afspraken tot stand volgens het standaard proces voor komen tot afspraken. Echter dient de eerste input voor specifieke afspraken ten allen tijde te komen uit voorbeelden uit de praktijk en geopperd door partijen die sleutelrollen in het DSGO (zullen) vervullen. Hiermee wordt geborgd dat specifieke afspraken de praktijk ondersteunen en gebruikt worden. Vervolgens wordt deze input meegenomen in het standaard proces voor komen tot afspraken.

Voor meer informatie zie deze pagina's:

Aanpak ontwikkeling van het Afsprakenstelsel DSGO

Hoe verhoudt semantiek zich tot het afsprakenstelsel DSGO?

Wanneer data wordt gedeeld is een gedeeld begrip van de semantiek van de gedeelde data essentieel. Het DSGO is gericht om data delen te realiseren in de gehele gebouwde omgeving. Waar in de ene situatie met BIM-modellen wordt gewerkt, gaat het in een andere situatie over product data. Wanneer in het afsprakenstelsel afspraken over semantiek worden opgenomen zijn dit specifieke afspraken.

Voor meer informatie zie deze pagina's:

Scope van het Digitaal Stelsel Gebouwde Omgeving

Aanpak ontwikkeling van het Afsprakenstelsel DSGO

Hoe werkt een datadienst?

Hebben we praktische voorbeelden van het DSGO?

Twee verhalen zijn uitgewerkt als praktisch voorbeeld van use cases mogelijk met het toekomstig DSGO.

1. Delen van product data als voorbeeld case
2. Delen van planningsdata in een bouwhub als voorbeeld case

Verder is het DSGO-programma bezig met het realiseren van concrete use cases. Wanneer deze use cases verder ontwikkeld worden wordt dit publiekelijk gecommuniceerd. Zie bijvoorbeeld dit artikel over de ontwikkeling van verschillende use cases ondersteunt door het DSGO-programma.

Wat houdt een abonnement op een gebeurtenis in?

Een abonnement op een gebeurtenis is een gestandaardiseerde datadienst die de partij (die zich op voorhand heeft geabonneerd op meldingen over een (type) gebeurtenis) inlicht over deze gebeurtenis. Een abonnement speelt een belangrijke rol wanneer een datadienstgebruiker (met toestemming van de rechthebbende) op de hoogte gehouden wil worden van gebeurtenissen (bijvoorbeeld wijzigingen van de brondata) door middel van notificaties van de datadienstaanbieder op bepaalde resources. Datadienstaanbieders zijn niet verplicht een abonnement te implementeren.

Voor meer informatie zie de pagina:

Abonnement op een gebeurtenis

Wat is het verschil tussen autoriseren en delegeren?

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. In het afsprakenstelsel is het onderwerp van autorisatie gesplitst in het autorisatiebeleid opstellen, autorisatie-

informatie organiseren, en het autorisatiebesluit nemen. Voor elke datadienst moet een autorisatiebesluit worden genomen. Om dit te doen moet de datadienstaanbieder autorisatie informatie toetsen tegen het autorisatiebeleid. .

Delegatie is het overdragen van een bevoegdheid aan een ander die de bevoegdheid gaat uitoefenen. Binnen het DSGO kan de rechthebbende haar gebruikersrechten over data delegeren. Wanneer er sprake is van delegatie is informatie over gedelegeerde rechten benodigde autorisatie-informatie die getoetst moet worden tegen het autorisatiebeleid.

Voor meer informatie zie deze pagina's:

Autorisatiebeleid opstellen

Autorisatie-informatie organiseren

Delegaties

Autorisatiebesluit nemen

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 o.a wie de rechthebbende is, tot welke (delen van) datadiensten rechthebbende gerechtigd zijn en of het mogelijk is om rechten te delegeren aan derde partijen.

Als het mogelijk is om rechten te delegeren, dan mag de rechthebbende binnen de kaders van de toegangscontroleregels besluiten onder welke voorwaarden zij rechten delegeert aan een gedelegeerde datadienstgebruiker.

Voor meer informatie zie de pagina's:

Autorisatie

Autorisatiebeleid opstellen

Hoe wordt bepaald wie de rechthebbende is?

De rechthebbende is de partij die gebruiksrechten heet over data en zeggenschap heeft over de gebruikersrechten van derde partijen betreffend die data. Welke partij gebruiksrechten over data heeft (en dus rechthebbend is) kan voortvloeien uit wet- en regelgeving en/of contractuele afspraken. Wanneer wet- en regelgeving over desbetreffende data ontbreekt en er geen contractuele afspraken zijn is in praktijk vaak de partij waarbij data opgeslagen is rechthebbende.

Er kunnen meerdere entiteiten rechthebbend zijn over dezelfde data.

Voor meer informatie zie de pagina:

Het DSGO rollenmodel

Is een autorisatieregister vereist?

Een autorisatieregister is een mogelijke implementatie voor het registreren van delegaties. Delegatie is het overdragen van een bevoegdheid, van de rechthebbende, aan een ander die vervolgens die bevoegdheid kan gebruiken. Delegaties moeten worden vastgelegd voordat ze tijdens een datadienst kunnen worden gebruikt. In het DSGO zijn er meerdere manieren waarop de rechthebbende delegaties kunnen worden geregistreerd: De rechthebbende beheert zelf delegaties, de rechthebbende registreert zijn delegaties bij de datadienstaanbieder of de rechthebbende registreert zijn delegaties bij een onafhankelijk autorisatieregister.

Voor meer informatie zie de pagina:

Autorisatie-informatie organiseren

Waarom voorziet het afsprakenstelsel meerdere door de markt geleverde autorisatieregisters?

Autorisatieregisters worden door de markt ontworpen om innovatie te stimuleren en omdat autorisatieregisters specifieke kenmerken hebben afhankelijk van de use case of het deel van de keten waarvoor het autorisatieregister opereert. Vanwege dit specifieke karakter

is die rol beter belegd bij marktpartijen. Daarnaast heeft niet elke use case een autorisatieregister nodig voor de opslag van delegaties, dit kan ook bij de rechthebbende of bij de datadienstaanbieder.

Voor meer informatie zie de pagina's:

Autorisatie-informatie organiseren

Delegaties

Op welke wijze commiteren partijen zich juridisch aan het DSGO?

Deelnemers van het DSGO (datadienstaanbieders en marktvoorzieningen) sluiten een deelname-overeenkomst met de beheerorganisatie DSGO. Middels de deelnameovereenkomst wordt het afsprakenstelsel van toepassing verklaard waarmee een partij zich committeert aan de rechten en plichten die voor de te vervullen rol zijn opgesteld.

Partijen die geen deelnemer zijn (datdienstgebruikers en rechthebbenden) sluiten geen overeenkomst met de beheerorganisatie DSGO. Wanneer niet deelnemende partijen betrokken zijn bij een datadienst verklaren zij middels een overeenkomst met een deelnemer (datadienstaanbieder of marktvoorziening) de gebruikersvoorwaarden van het DSGO van toepassing. Met het accepteren van de gebruiksvoorwaarden committeren deze partijen zich aan de rechten en plichten voor de rol die ze vervullen zonder dat ze deelnemer hoeven te worden.

Zie voor meer informatie de pagina:

Juridische bepalingen

Wat kan de sector doen om nu al gebruik te maken van het DSGO?

Het DSGO is in een fase waar technische specificaties geïmplementeerd kunnen worden om datadiensten uit te voeren. De komende maanden wordt het DSGO doorontwikkeld naar een meer volwassen stelsel waarin meer functionaliteiten mogelijk worden. Ondertussen is het DSGO met verschillende use cases bezig om datadiensten op basis van het DSGO te realiseren.

Voor meer informatie zie de pagina

Aanpak ontwikkeling van het Afsprakenstelsel DSGO

Hoe wordt het DSGO beheert?

Tijdens de looptijd van het DSGO-programma wordt het afsprakenstelsel beheert door het DSGO projectteam Afsprakenstelsel. In een apart project binnen het DSGO-programma, worden de toekomstige governance en processen van het DSGO uitgewerkt waar de beheerorganisatie DSGO onderdeel van is.

Voor meer informatie zie deze pagina's:

Beheer

Governance

Hoe worden partijen uit de sector betrokken bij de governance van het DSGO?

De toekomstige governance van het DSGO bestaat uit een vertegenwoordiging van de sector & deelnemers, de beheerorganisatie DSGO en eventuele uitvoeringsorganisaties. Vertegenwoordiging uit de sector krijgt invulling middels een Gebruikersraad (GR) en een Change Advisory Board (CAB) beide bestaande uit deelnemers van het DSGO.

De Gebruikersraad borgt betrokkenheid van deelnemers op strategisch niveau door inhoudelijke besluiten over beheer, adoptie & doorontwikkeling van het DSGO. De Change Advisory Board adviseert over het aanpassen en uitbreiden van het DSGO en keuzes omtrent beheer & adoptie.

Voor meer informatie zie de pagina's:

Governance

Gebruikersraad

Change Advisory Board

## Bijlage

**DSGO voorbeel… tie.pdf**
27 Oct 2023, 09:32 am

**DSGO voorbeel… ata.pdf**
27 Oct 2023, 09:32 am