

Afsprakenstelsel DSGO	4
Introductie	7
Aanleiding Programma Digitaal Stelsel Gebouwde Omgeving	8
Doel van het Digitaal Stelsel Gebouwde Omgeving	9
Scope van het Digitaal Stelsel Gebouwde Omgeving	12
Het BLOFT-raamwerk	14
Illustratieve voorbeelden van het DSGO	15
Aanpak ontwikkeling afsprakenstelsel DSGO	16
Richtinggevende Principes	18
Principe 1: Vertrouwd	19
Principe 2: Breed toepasbaar	20
Principe 3: Toekomstbestendig	21
Principe 4: Inclusief	22
Principe 5: Kostenefficiënt	23
Principe 6: Gebaseerd op open standaarden	24
Principe 7: Schaalbaar	25
Principe 8: Doelmatig	26
Principe 9: Soeverein	27
Beheer	28
Leeswijzer (Reading Guide)	29
Eisen Notatieconventies(Requirements Notational Conventions)	30
Typografie (Typography)	31
Taal (Language)	32
Versiebeheer	33
Kern van het Afsprakenstelsel	35
Wat is een datadienst?	36
Datadienstdefinitie	37
Hoe werkt een datadienst?	39
Rollenmodel	40
Generiek Ondersteunende Functionaliteiten	44
Abonnement op een Datadienst	45
Datadienst ontdekking	47
Identificatie, Authenticatie en Autorisatie	48
Specifieke Functionaliteiten	49
Generieke Afspraken	50
API Specifications	51
Generic API Requirements	52
API Service Content	54
Data Service Resource	55
/subscriptions	56
Lifecycle of a Subscription	58
GET /subscriptions	59
POST /subscriptions	61
GET /subscriptions/{id}	63
DELETE /subscriptions/{id}	65

POST /subscriptions/{id}/test	67
/notifications	69
POST /notifications	71
/token	73
POST /token	74
POST /token/revoke	77
Generieke Technische Standaarden	80
RESTful API's	81
HTTP(s)	84
JSON	87
UTC	88
Identificatie	89
Identificatie van Organisaties	91
Identificatie van Personen	92
Authenticatie	93
Authenticatie op Transport Niveau	94
Authenticatie op Datadienst Niveau	95
Machine to Machine Authenticatie	96
Human to Machine Authenticatie	97
Betrouwbaarheidsniveau (Level of Assurance)	98
Autorisatie	99
Autorisatiebeleid	100
Autorisatiebeheer	101
Autorisatiebesluit	102
Grofmazig en fijnmazige autorisatie	103
Grofmazig M2M Autorisatie Flow	104
Informatiebeveiliging	106
Transport Layer Security	107
JSON Web Tokens (JWT)	109
Ondertekening	113
Juridische Context	114
Mededingingsrecht	115
Algemene Verordening Gegevensbescherming (AVG)	116
Electronic Identification and Trust Services (eIDAS)	118
Europa's data strategie (overkoepelend Europees beleid)	119
Data governance verordening (DGV)	120
Data verordening (DV)	121
Domein specifieke wet-en regelgeving	122
Service Level Agreements	123
SLAs voor Datadienstaanbieders	124
SLAs voor de Beheerorganisatie	127
Incidentenbeheer	128
Marktvoorzieningen	130
Specifieke Afspraken	131
Appendix	132

Overzicht van Eisen	133
Begrippenlijst (Glossary)	143
FAQ	152

Afsprakenstelsel DSGVO

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



Introductie

- In de [Introductie](#) vind je meer informatie over DigiGO, DSGVO, en de aanleiding, het doel, scope en Richtinggevende Principes van het afsprakenstelsel DSGVO.
- In [Versie Beheer](#), vind je een overzicht van alle voorgaande en geplande releases.
- In [Kern van het Afsprakenstelsel](#) 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.

Inhoudsopgave

- ▼ [Introductie](#)
 - [Aanleiding Programma Digitaal Stelsel Gebouwde Omgeving](#)
 - ▼ [Doel van het Digitaal Stelsel Gebouwde Omgeving](#)
 - [Scope van het Digitaal Stelsel Gebouwde Omgeving](#)
 - [Het BLOFT-raamwerk](#)
 - [Illustratieve voorbeelden van het DSGVO](#)
 - [Aanpak ontwikkeling afsprakenstelsel DSGVO](#)
 - ▼ [Richtinggevende Principes](#)
 - [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
- Beheer
- ▼ Leeswijzer (Reading Guide)
 - Eisen Notatieconventies(Requirements Notational Conventions)
 - Typografie (Typography)
 - Taal (Language)
- Versiebeheer
- ▼ Kern van het Afsprakenstelsel
 - ▼ Wat is een datadienst?
 - Datadienstdefinitie
 - Hoe werkt een datadienst?
 - Rollenmodel
 - ▼ Generiek Ondersteunende Functionaliteiten
 - Abonnement op een Datadienst
 - Datadienst ontdekking
 - Identificatie, Authenticatie en Autorisatie
 - Specifieke Functionaliteiten
- ▼ Generieke Afspraken
 - ▼ API Specifications
 - Generic API Requirements
 - API Service Content
 - Data Service Resource
 - › /subscriptions
 - › /notifications
 - › /token
 - ▼ Generieke Technische Standaarden
 - RESTful API's
 - HTTP(s)
 - JSON
 - UTC
 - ▼ Identificatie
 - Identificatie van Organisaties
 - Identificatie van Personen
 - ▼ Authenticatie
 - Authenticatie op Transport Niveau
 - › Authenticatie op Datadienst Niveau
 - ▼ Autorisatie
 - Autorisatiebeleid
 - Autorisatiebeheer
 - › Autorisatiebesluit
 - ▼ Informatiebeveiliging
 - Transport Layer Security
 - › JSON Web Tokens (JWT)
 - ▼ Juridische Context
 - Mededingingsrecht
 - Algemene Verordening Gegevensbescherming (AVG)
 - Electronic Identification and Trust Services (eIDAS)
 - › Europa's data strategie (overkoepelend Europees beleid)
 - Domein specifieke wet-en regelgeving

- Service Level Agreements
 - SLAs voor Datadienstaanbieders
 - SLAs voor de Beheerorganisatie
- Incidentenbeheer
- Marktvoorzieningen
- Specifieke Afspraken
- ▼ Appendix
 - Overzicht van Eisen
 - Begrippenlijst (Glossary)
 - FAQ

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

i 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. Deze versie van het afsprakenstelsel is het resultaat van de eerste publieke review. 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.

Bijlage



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. Deze versie van het afsprakenstelsel is het resultaat van de eerste publieke review. Op dit moment is het niet mogelijk om op deze versie opmerkingen te geven. 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](#)
- › [Doel van het Digitaal Stelsel Gebouwde Omgeving](#)
- * [Aanpak ontwikkeling afsprakenstelsel DSGO](#)
- › [Richtinggevende Principes](#)
- * [Beheer](#)
- › [Leeswijzer \(Reading Guide\)](#)

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 [programmplan](#).

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.

:Q

uot **Bron:** Programma Plan DSGO - [1.2 Visie en doelstelling DSGO-programma](#)

es:

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 (nog te selecteren) [beheerorganisatie](#).

Doel van het Digitaal Stelsel Gebouwde Omgeving

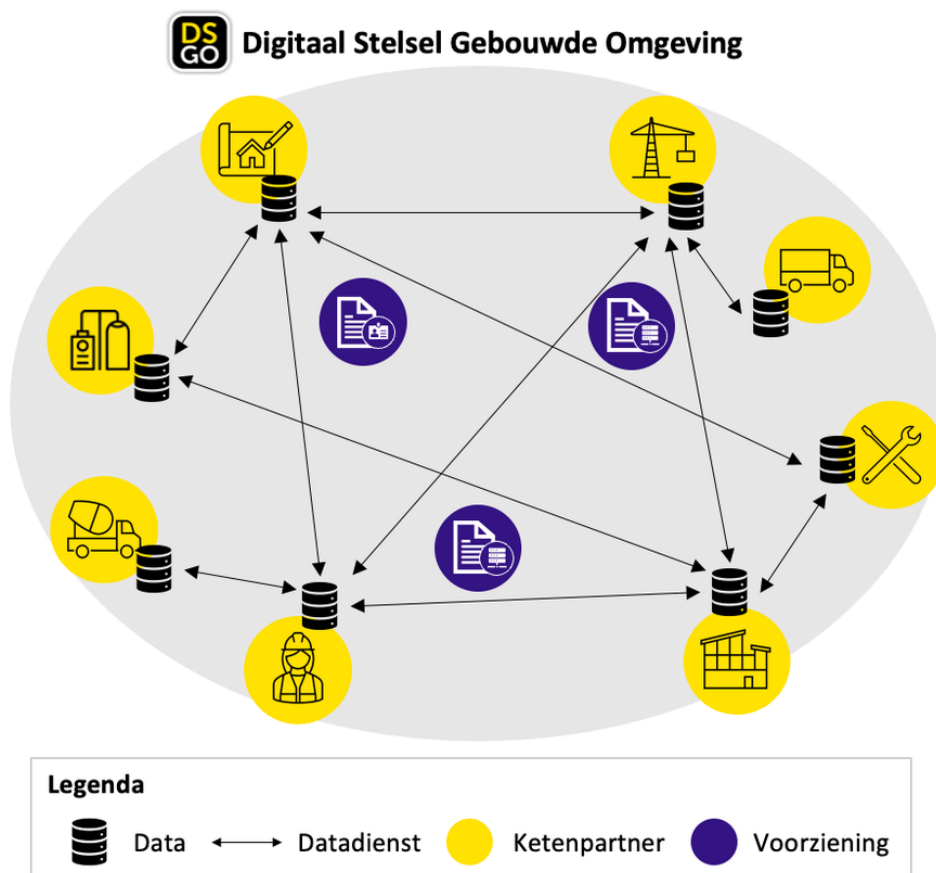
Het **doel** van het **DSGO-programma** is het ontwerpen, realiseren en in beheer (doen) nemen van het **Digitaal Stelsel Gebouwde Omgeving (DSGO)**. Het DSGO faciliteert een netwerk van **datadiensten** om in de gebouwde omgeving **data te delen** en/of te bewerken in een **federatief ecosysteem** o.b.v.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

- Het **afsprakenstelsel DSGO** biedt afspraken om op gestandaardiseerde wijze datadiensten te implementeren.
- Stelselvoorzieningen 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 deelnemende 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 voorwaarde 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.

:Q

uot Bron: Logius - [Wat is een Afsprakenstelsel?](#)

es:

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.”

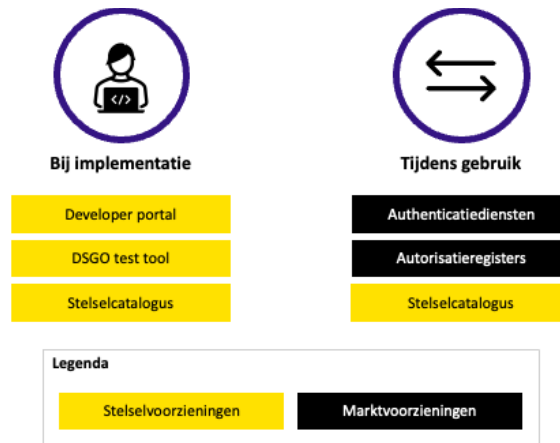


De scope van het afsprakenstelsel DSGO wordt verder gedetailleerd op de onderliggende pagina. Verder vormt het BLOFT-raamwerk (geformuleerd door de [Data Sharing Coalition](#) in het [Data Sharing Canvas](#)) het startpunt voor het maken van afspraken die binnen het afsprakenstelsel opgenomen worden. 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 de implementatie en bij gebruik van het DSGO.

De minimale vereisten aan alle voorzieningen worden gedefinieerd gedurende de ontwikkeling van het DSGO. Alle voorzieningen staan onder toezicht van de [beheerorganisatie van het DSGO](#). Voorzieningen die door de [beheerorganisatie van het 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 van belang zijn

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

Stelselvoorzieningen

- Developer portal: Interface voor het ontwikkelen van technische implementaties van DSGO voor ICT-ontwikkelaars.
- DSGO test tool: Technische tool voor het valideren van de functionaliteit van implementaties gebaseerd op het afsprakenstelsel DSGO.
- **Stelselcatalogus**: Catalogus die alle nodige informatie bevat om datadiensten, deelnemers, en stelselvoorzieningen te vinden, begrijpen en gebruiken.

Marktvoorzieningen

- **Authenticatiediensten** en **autorisatieregisters**: Optionele diensten voor gemeenschappelijk gebruik die **identificatie**, **authenticatie** en **autorisatie** 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.

i Op dit moment volgt het DSGO iSHARE voor alle eisen van marktvoorzieningen. Voor meer informatie over Authenticatiediensten (Identity providers) en autorisatieregisters (Authorization registry) zie **iSHARE**.

Scope van het Digitaal Stelsel Gebouwde Omgeving

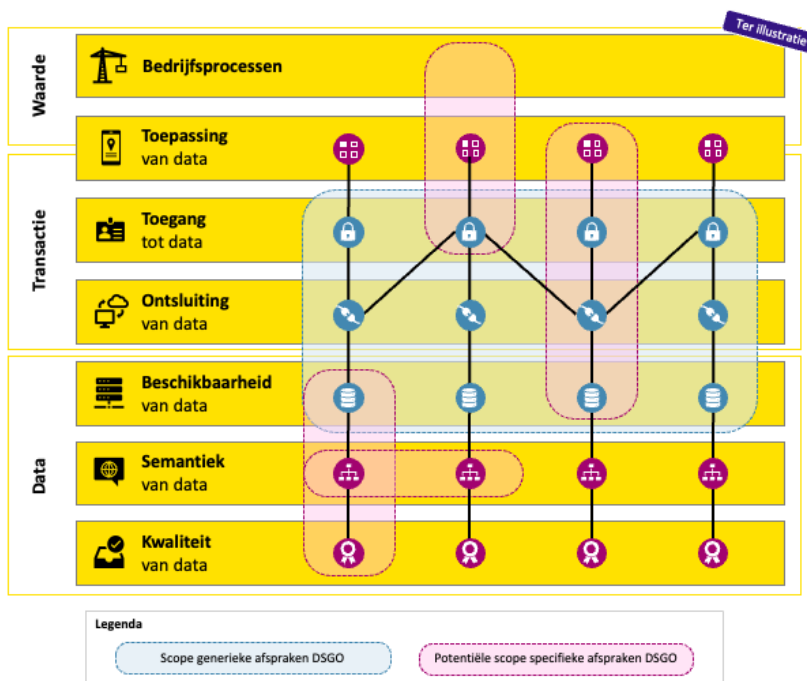
In de gebouwde omgeving wordt in ketens waarde gecreëerd door en voor diverse partijen. Daartoe voeren (keten)partijen activiteiten uit in bedrijfsprocessen (zowel intern als tussen ketenpartijen), gebruikmakend van bedrijfsspecifieke applicaties. Om het doel van de applicaties te bereiken wordt in deze 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 zijn data agnostisch, en ondersteunen daarmee alle mogelijke **datadiensten**, onafhankelijk 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 use cases (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

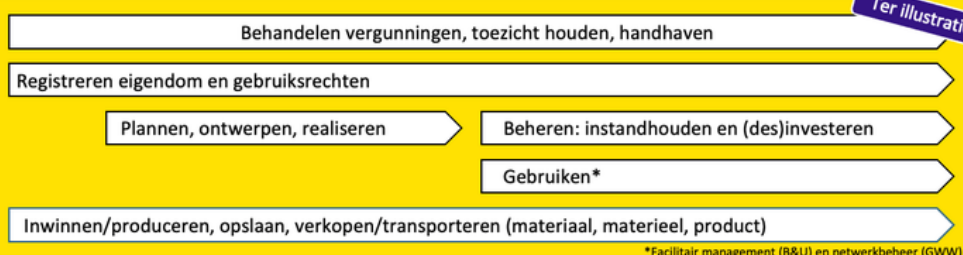
In het onderstaande voorbeeld worden enkele voorbeeld bedrijfsapplicaties getoond die gebruikt worden in verschillende bedrijfsprocessen.

Ter illustratie

Waarde



Bedrijfsprocessen



*Faciliteit management (B&U) en netwerkbeheer (GWW)

Transactie

Toepassing van data



Toegang tot data



Ontsluiting van data

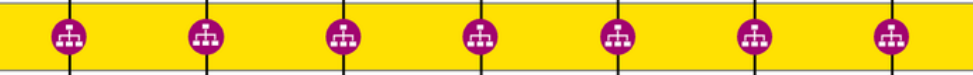


Data

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](#).

BUSINESS	LEGAL	OPERATIONAL	FUNCTIONAL	TECHNICAL Indicatief
Context & doelen <ul style="list-style-type: none"> • Visie & missie • Business rationale • Tweezijdige markten & Netwerk effecten • Rictingevende principes • Waardeproposities 	Relevante wet- en regelgeving <ul style="list-style-type: none"> • Relevante wetgeving • Toezichhoudende organen • Gebruik van standaarden • Privacy 	Operationele governance <ul style="list-style-type: none"> • Certificeringsprocessen • Escalaties & beslissingsbevoegdheid • Marketing & adoptie 	Functionele scope <ul style="list-style-type: none"> • Services • Functionele componenten • Authenticatie • Autorisatie • Data delen • Datakwaliteit • Toegangsduur 	Technische specificaties <ul style="list-style-type: none"> • Data uitwisseling protocollen/standaarden • Berichten formats • Data formats • Error afhandeling
Rollen & verantwoordelijkheden <ul style="list-style-type: none"> • Rechthebbende • Datadienstgebruiker • Datadienstaانبieder • Uitbesteding • Routing • Andere rollen 	Contracten <ul style="list-style-type: none"> • Stelseldeelname • Bilaterale deelnameovereenkomsten • Algemene voorwaarden • Deelname criteria & KYC • Aansprakelijkheid 	Risicomanagement <ul style="list-style-type: none"> • Risicobereidheid • Risico analyse/score 	Interactiemodel <ul style="list-style-type: none"> • Dienstontdekking • Customer Journey • Functionele flow • Data flow 	Beveiliging <ul style="list-style-type: none"> • Betrouwbaarheid • Integriteit • Onweerlegbaarheid • Authenticiteit • Fraude detectie & monitoring • Pen-testing
Vergoedingen <ul style="list-style-type: none"> • Compensatievoorwaarden • Afsprakenstelsel financiering 	Governance <ul style="list-style-type: none"> • Samenstelling & toezicht • Governancestructuur • Certificering • Sancties 	Incidentmanagement <ul style="list-style-type: none"> • Incidentenbeheer • Communicatie 	Gebruikerservaring <ul style="list-style-type: none"> • UX standaardisatie • Scherm vereisten • Kanalen (Internet/mobiel/...) 	Informatiemanagement <ul style="list-style-type: none"> • Auditing • Loggen • Archivering • Verslagleggingvereisten
Branding <ul style="list-style-type: none"> • Branding • Stijlgids • Marketing richtlijnen 		Verandermanagement <ul style="list-style-type: none"> • Verandermanagement procedures & processen • Versiebeheer 	Privacy <ul style="list-style-type: none"> • Regie op gegevens • Data minimalisatie • Herleidbaarheid • Identificatie • Blindness • Domein specifieke privacy 	
		Service levels <ul style="list-style-type: none"> • Beschikbaarheid en prestatie • Onderhoudsvensters • Monitoring & verslaglegging 		
		Tooling <ul style="list-style-type: none"> • Documentmanagement • Notificatie platform • Stelselcatalogus • Test-tooling/scripten • Software bibliotheken • Issue-tracker 		

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.

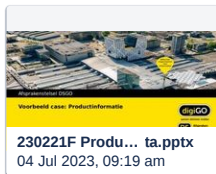
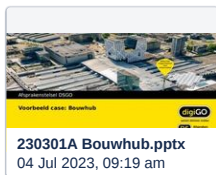
Illustratieve voorbeelden van het DSGO

Er zijn twee verhalen zijn uitgewerkt als praktisch voorbeeld van use cases mogelijk met het toekomstig 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.

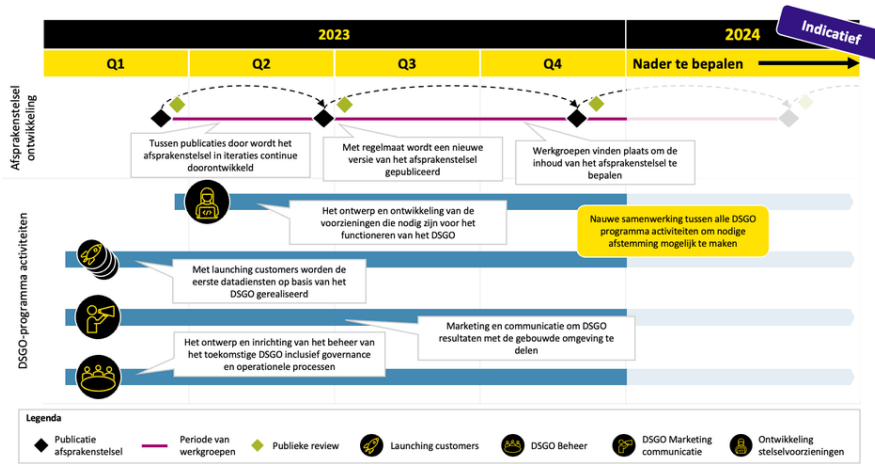
Bijlage



Aanpak ontwikkeling afsprakenstelsel DSGO

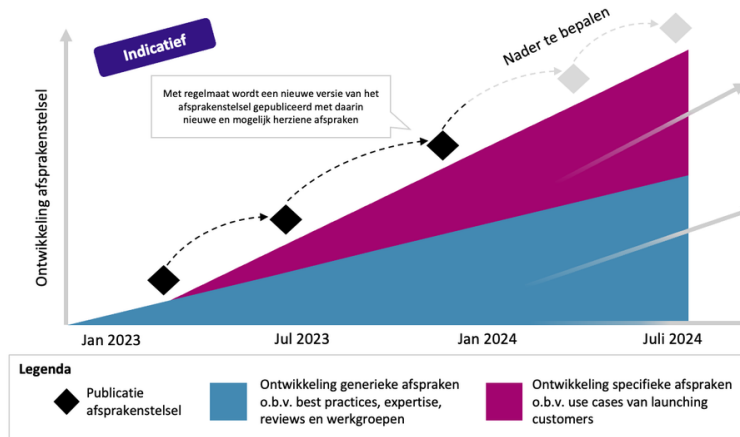
Voor opmerkingen over het afsprakenstelsel DSGO, plaats je opmerking in [deze excel sheet](#) en stuur deze naar afsprakenstelseldsgo@digigo.nu

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 launching customers, 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 continu worden ontwikkeld 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.

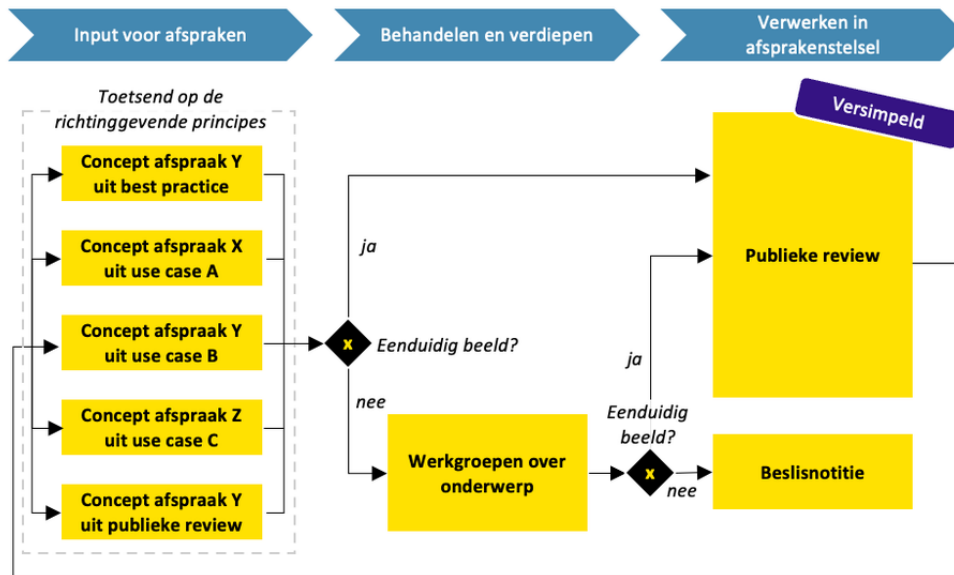


Generiek en specifieke afspraken in het afsprakenstelsel worden iteratief ontwikkeld

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 geagendeerd wordt in werkgroepen, publieke reviews en inzichten uit use cases van launching customers. 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.

Proces voor het komen tot afspraken

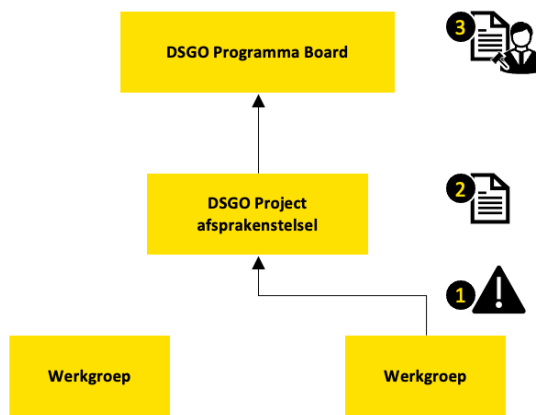
Om tot een overeenstemming te komen over de inhoud van de generieke en specifieke afspraken in het afsprakenstelsel wordt een standaard proces gevolgd, zoals geschetst in de onderstaande figuur. De eerste concept afspraken worden opgesteld op basis van best practices, use cases, en de resultaten van publieke review. Hieruit ontstaan onderwerpen die ter discussie worden gesteld. Voor deze onderwerpen worden werkgroepen georganiseerd om het onderwerp te verdiepen. Bij deze werkgroepen is het noodzakelijk dat de juiste stakeholders en experts uit de sector betrokken zijn. Het resultaat van deze onderwerpen wordt opgenomen in het afsprakenstelsel en behandeld in een volgende iteratie van een publieke review.



Middels werkgroepen wordt een eenduidig beeld over de inhoud van afspraken bepaald en worden deze verwerkt in het afsprakenstelsel.

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:
 - o Keuzeopties
 - o Afwegingen per optie
 - o Reden waarom de keuze niet gemaakt kon worden
 - o 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.

Bijlage



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 afsprakenstelseldsgo@digigo.nu of een van de projectteam leden.

In een [apart project](#) binnen het DSGO-programma, wordt de governance en processen van de toekomstige [beheerorganisatie DSGO](#) uitgewerkt. De beheerorganisatie van het DSGO definieert en beheert het [DSGO](#). Dit bevat het zorgen voor de doorontwikkeling van het [afsprakenstelsel](#), toezien op de naleving, toezien op de operatie van [stelselvoorzieningen](#) en beslechten van geschillen. Hiermee borgt de beheerorganisatie het beheer en doorontwikkeling van het DSGO.

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 gebruik 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 weergegeven. 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 verboden 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,

:Q

uot 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

Datum	Beschrijving	Status	Link
oktober 2023		GEPLAND	
04 juli 2023	<p>De opmerkingen die zijn gemaakt op de vorige versie en het resultaat van de publieke review zijn verwerkt.</p> <p>Voor de verwerkte schriftelijke review, zie deze excel sheet.</p> <p>Voor de discussiepunten van de Tech-Xperiment van de publieke review, zie dit document.</p> <p>Voor de discussiepunten van de Functionele werk van de publieke review, zie dit document.</p> <p>Voor de discussiepunten van de juridische publieke review van de publieke review, zie dit document.</p>	BESCHIKBAAR	 Afsprakenstelsel DSGVO
26 mei 2023	<p>Publicatie van het afsprakenstelsel DSGVO ten behoeve van de publieke review op 15 juni 2023. Onderwerpen doorontwikkeld:</p> <ul style="list-style-type: none"> • Wat is een datadienst? • Authenticatie • Autorisatie • Informatiebeveiliging 	BESCHIKBAAR	Afsprakenstelsel DSGVO 26 mei 2023
31 maart 2023	<p>Eerste publieke publicatie van het afsprakenstelsel DSGVO.</p> <p>De opmerkingen die zijn gemaakt op de vorige versie en het resultaat van de thematafels zijn verwerkt.</p> <p>Voor de verwerkte schriftelijke review, zie deze excel sheet.</p> <p>Voor de discussiepunten van de Technische thematafel van de publieke review, zie dit document.</p> <p>Voor de discussiepunten van de Organisatie en Proces thematafel van de publieke review, zie dit document.</p> <p>Voor de discussiepunten van de Juridische thematafel van de publieke review, zie dit document.</p>	BESCHIKBAAR	Afsprakenstelsel DSGVO 31 maart 2023
16 februari 2023	<p>Publicatie van het afsprakenstelsel DSGVO ten behoeve van de publieke review van het afsprakenstelsel.</p>	REVIEWED	Afsprakenstelsel DSGVO 16 februari 2023


Bijlage




Opmerkingen A...04.xlsx
06 Jul 2023, 03:31 pm



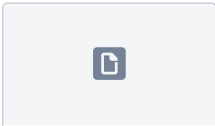
230615 verslagl... ent.pdf
06 Jul 2023, 02:25 pm




230615 Functio... -up.pdf
05 Jul 2023, 02:57 pm




230615 Resulta... ent.pdf
04 Jul 2023, 11:38 am



Failed to load



Opmerkingen A...31.xls
04 Jul 2023, 09:14 am



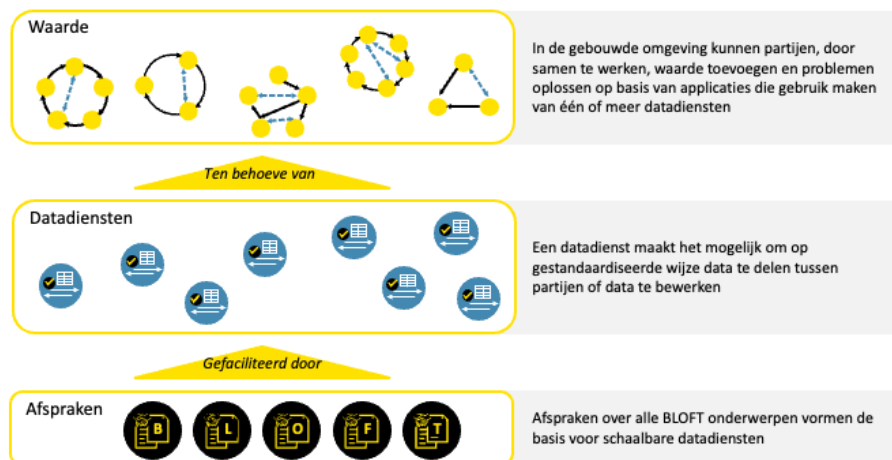
230615 Resulta... iew.pdf
04 Jul 2023, 11:38 am

Kern van het Afsprakenstelsel

i In de [introdactie](#) zijn de [aanleiding](#) en [doel van het DSGVO](#), 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 te 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 voor bepaalde datadiensten van toepassing zijn om op makkelijk op te kunnen schalen binnen de gebouwde omgeving. Dit zijn afspraken die bovenop de generieke functionaliteiten zijn gemaakt om sector-, keten-, of oplossings specifieke 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?](#)
- [Rollenmodel](#)
- › [Generiek Ondersteunende Functionaliteiten](#)
- [Specifieke Functionaliteiten](#)

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 moet dan een datadienst zelf vormgeven en binnen de voorwaarden van het afsprakenstelsel een datadienst definiëren. 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](#).

:Q

uot **Bron:** DCAT v3 - [Abstract](#)

es:

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 identificer	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 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)

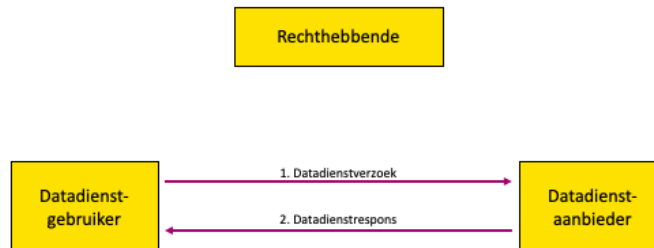
Service level agreements (SLAs)	Alle service level agreements over de dienstverlening of prestatiegaranties gerelateerd aan de datadienst.(bv. garanties inzake uptime of reactietijd)
---------------------------------	--

! **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 interactie 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 de voorwaarden 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 een **API (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
Create	De datadienstgebruiker stuurt data naar de datadienstaanbieder die op basis hiervan een data resource aanmaakt.
Read	De datadienstgebruiker ontvangt de gevraagde data resource van de datadienstaanbieder.
Update	De datadienstgebruiker stuurt data naar de datadienstaanbieder die op basis hiervan een data resource bijwerkt.
Delete	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.

Rollenmodel

Rollen in een [datadienst](#) worden gedefinieerd door de rechten, verplichtingen en verwachte interacties van een partij. Binnen de volledige context van het [afsprakenstelsel](#) zijn enkele rollen die nodige functionaliteiten bieden voor het uitvoeren van datadiensten en het opereren van het [DSGO](#). De rollen worden geclassificeerd als rollen die direct bij elke datadienst actief betrokken zijn, en rollen die ondersteunen en mogelijk (indirect) betrokken zijn bij een datadienst. Deze zijn hieronder beschreven:

Rollen direct betrokken bij een datadienst:

- [Datadienstaanbieder](#)
- [Datadienstgebruiker](#)
- [Rechthebbende](#)

Ondersteunende rollen:

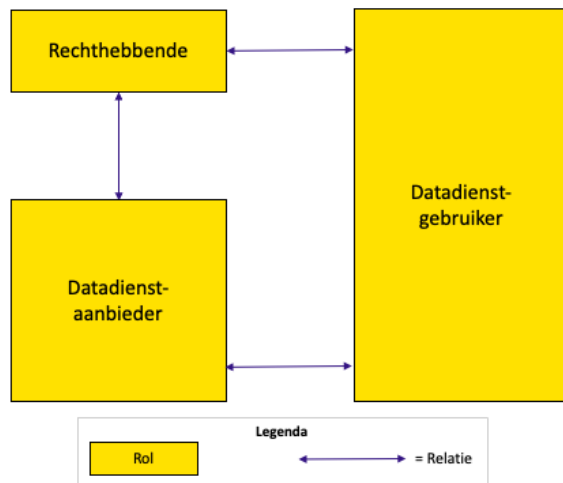
- [Autorisatieregister](#)
- [Authenticatiedienst](#)
- [Beheer](#)
- [Stelselcatalogus](#)

! **Merk op**, in de verdere door ontwikkeling van het afsprakenstelsel kunnen aanvullende rollen nodig worden geacht die hier zullen worden toegevoegd.

Rollen direct betrokken bij een datadienst

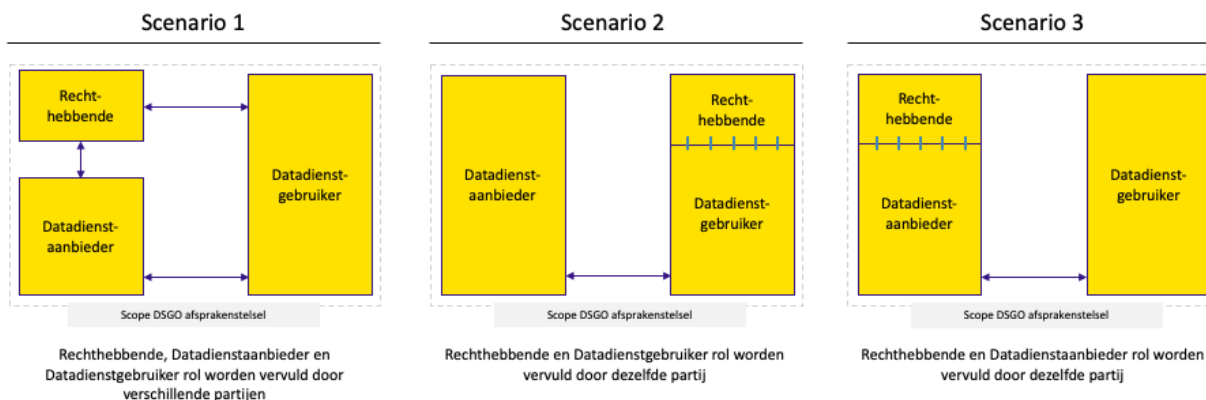
Bij elke datadienst zijn drie rollen actief betrokken, de datadienstaanbieder, de datadienstgebruiker en de rechthebbende. De rollen worden in de tabel gedefinieerd en in de afbeelding worden relaties weergegeven.

Rol	Omschrijving
Datadienstaanbieder	De datadienstaanbieder is de partij die de verantwoordelijkheid draagt voor het definiëren, aanbieden en het juist leveren van een datadienst.
Datadienstgebruiker	De datadienstgebruiker is de partij die de verantwoordelijkheid draagt voor het gebruiken van een aangeboden datadienst omdat dit waarde oplevert (bv. dienstverlening verbeteren of mogelijk maken)
Rechthebbende	De rechthebbende is de partij die rechten heeft over data en toegang kan verlenen aan derden



Drie rollen zijn actief direct betrokken bij elke datadienst

Een enkele partij kan meerdere rollen invullen bij elke datadienst. Bij een volgende datadienst kunnen dezelfde entiteiten een andere rol innemen. De scenario's zijn gevisualiseerd in het voorbeeld hieronder:



Eén partij kan tegelijk meerdere rollen vervullen

★ Voorbeeld van mogelijke invullingen van de rollen.

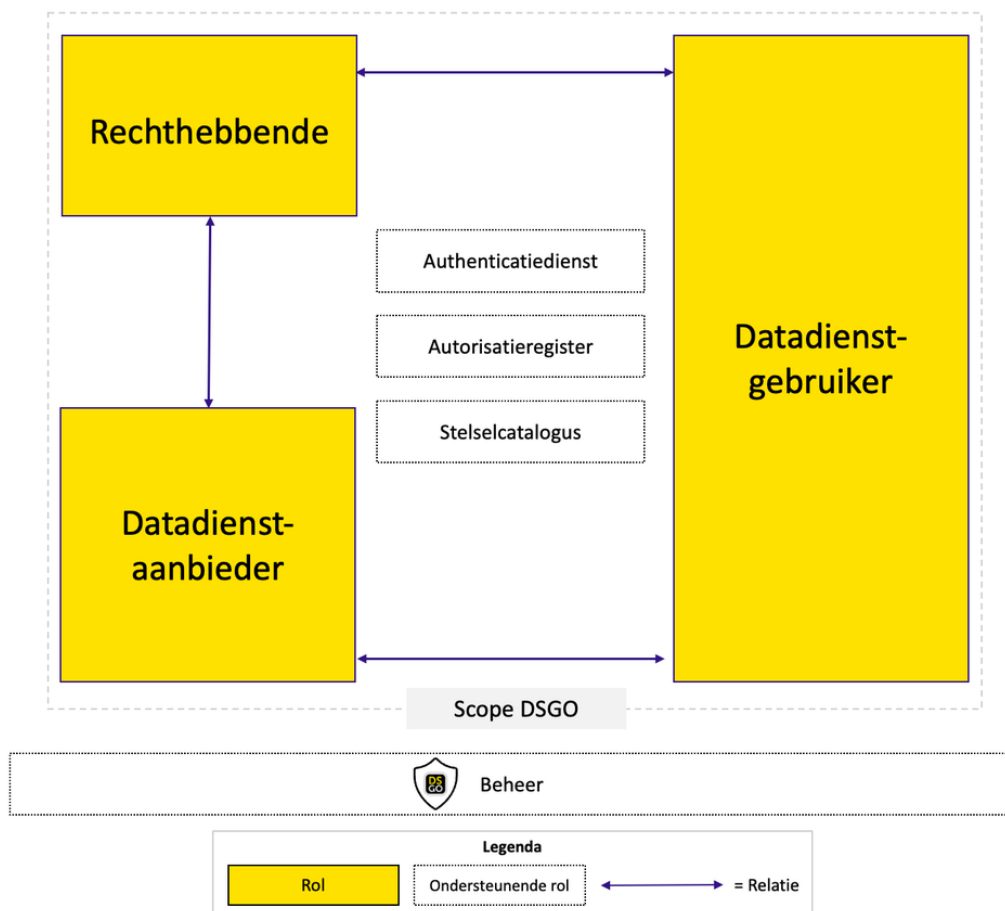
Scenario 1: Wanneer productinformatie bij een leverancier is opgeslagen kan de leverancier als datadienstaanbieder een datadienst met productinformatie (bijvoorbeeld de classificatie gegevens) aanbieden aan een aannemer, de datadienstgebruiker. Dit terwijl de fabrikant rechthebbende is over de productinformatie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

Scenario 2: 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.

Scenario 3: Wanneer de fabrikant, als datadienstaanbieder, productinformatie direct aanbiedt aan de aannemer, de datadienstgebruiker, is de fabrikant zowel datadienstaanbieder als rechthebbende.

Ondersteunende rollen

Naast de drie rollen direct betrokken bij een datadienst zijn er enkele ondersteunende rollen die optioneel betrokken kunnen zijn bij een datadienst en nodig zijn voor het functioneren van het DSGVO. De rollen zijn beschreven in de onderstaande tabel en de relaties zijn weergegeven in de afbeelding hieronder. Afhankelijk van de rollen die partijen aannemen, kunnen bepaalde rollen door verschillende partijen worden ingevuld, mogelijke invullingen worden in de tabel geduid.



Verschillende rollen ondersteunen het uitvoeren van een datadienst binnen het DSGO

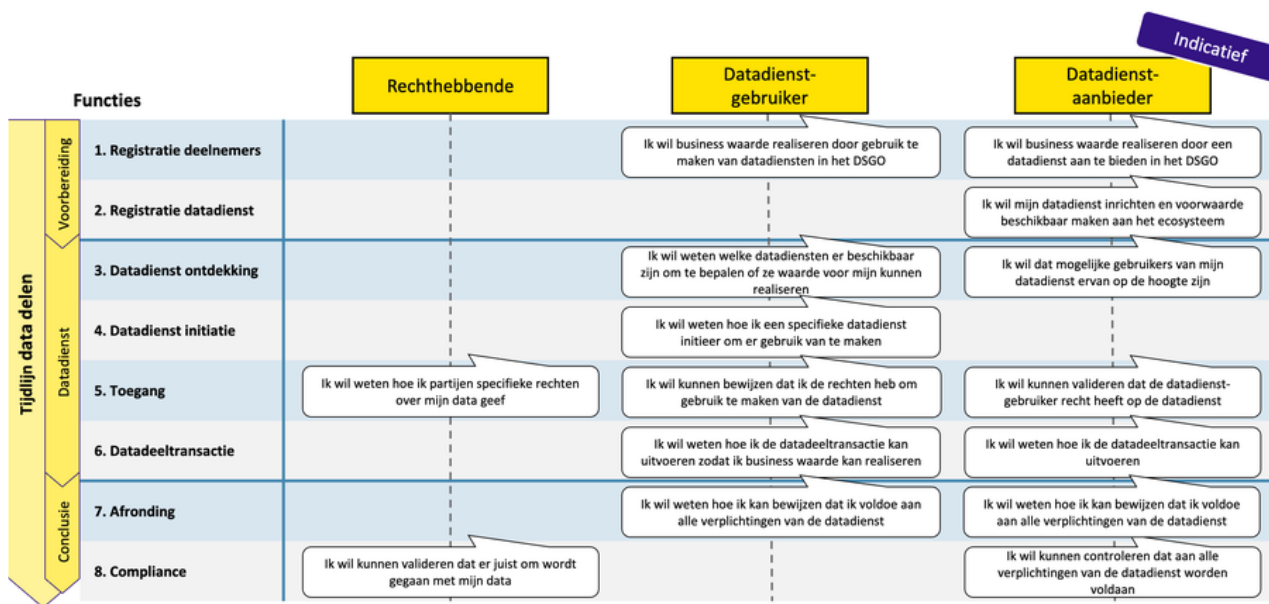
Merk op, in de verdere uitwerking van deze rollen zal de invulling van de verschillende ondersteunende rollen nog worden gedetailleerd.

Rol	Omschrijving	Opmerking
Authenticatiedienst	Een authenticatiedienst biedt diensten aan voor het creëren, onderhouden, beheren en valideren van identiteiten van personen ten behoeve van authenticatie voor partijen binnen het afsprakenstelsel.	De rol van een authenticatiedienst kan op twee manieren worden ingevuld: <ul style="list-style-type: none"> • Centraal gerealiseerd onder beheer van de beheerorganisatie • Door een onafhankelijke derde partij (technische dienstverlener)
Autorisatieregister	Een onafhankelijke vertrouwde partij die diensten biedt voor het registreren, opslaan en ontsluiten van autorisaties voor de toegang tot een datadienst.	Een autorisatieregister stelt de datadienstaanbieder en rechthebbende in staat om het beheer van autorisaties verstrekt door de rechthebbende uit te besteden aan een onafhankelijk vertrouwde partij indien nodig. Alternatieven voor het gebruik van een autorisatieregister zijn: <ul style="list-style-type: none"> • De rechthebbende die hun eigen autorisaties beheert en beschikbaar stelt aan de datadienstaanbieder. • De rechthebbende die hun autorisaties registreert direct bij de datadienstaanbieder
Beheer	Het beheer van het afsprakenstelsel zorgt voor de doorontwikkeling van het afsprakenstelsel, ziet toe op de naleving	Zal worden gerealiseerd door een te selecteren beheerorganisatie.

	ervan, en beslecht geschillen om data delen te ondersteunen.	
Stelselcatalogus	Een stelselcatalogus biedt diensten aan om informatie te verschaffen die nodig is om deelnemers , datadiensten, en voorzieningen te vinden , begrijpen en gebruiken.	De rol van een stelselcatalogus kan op meerdere manieren worden ingevuld: <ul style="list-style-type: none"> • In een catalogus dat beheerd wordt door de beheerorganisatie • Door een onafhankelijke derde partij (technische dienstverlener) • Decentrale implementatie

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 beiden (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 Datadienst](#)
- ° [Datadienst ontdekking](#)
- ° [Identificatie, Authenticatie en Autorisatie](#)

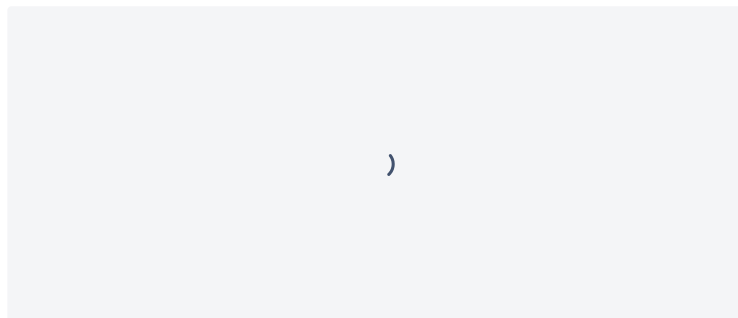
Voor alle generieke ondersteunende functionaliteiten zijn [generieke afspraken](#) opgesteld.

Abonnement op een Datadienst

Het concept van een [abonnement](#) is relevant voor veel partijen in de gebouwde omgeving. Daarom definieert het [DSGO](#) een abonnement als een gestandaardiseerde [datadienst](#). [Datadienstaanbieders](#) zijn niet verplicht een abonnement te implementeren. Een abonnement op een datadienst speelt een belangrijke rol wanneer een [datadienstgebruiker](#) (met toestemming van de [rechthebbende](#)) op de hoogte gehouden wil worden van [events](#) (gebeurtenissen, bijvoorbeeld wijzigingen) door notificaties van de datadienstaanbieder op bepaalde resources. Deze termen worden in de tabel hieronder beschreven.

Term	Omschrijving
Event	Een (door de datadienstaanbieder) gedefinieerde specifieke gebeurtenis in de systemen van een 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 specifieke events gerelateerd aan een datadienst.
Notificaties	Een melding van een event van de datadienstaanbieder, ontvangen door de datadienstgebruiker onder de voorwaarde van een abonnement.

In de figuur hieronder wordt het interactiemodel weergegeven hoe een abonnement tot stand komt en hoe notificaties van events worden doorgegeven.



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

#	Acties	Omschrijving
1	Abonneren verzoek	De datadienstgebruiker initieert het abonneren op een datadienst 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	Event	De datadienstaanbieder monitort de resource voor gebeurtenissen zoals beschreven in de abonnementsvoorwaarde.
4	Notificatie	De datadienstaanbieder stuurt de datadienstgebruiker een notificatie wanneer een event plaatsvindt.

Afhankelijk van het abonnement die de datadienstaanbieder gefineerd, kan de datadienstgebruiker kiezen om een actie te ondernemen (zoals het ophalen van aangepaste data) bij het ontvangen van de notificatie.

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.

! 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

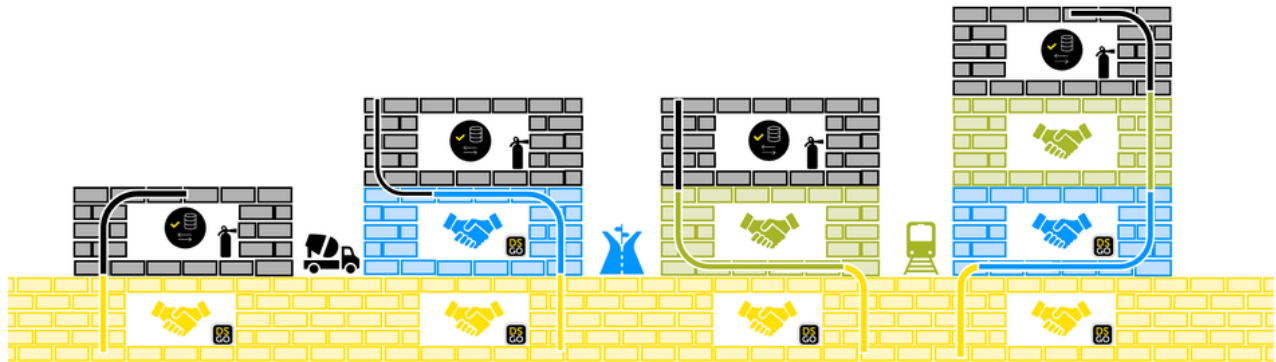
Binnen [het afsprakenstelsel](#) wordt 'Identity en Access Management' (IAM) gesplitst in de onderwerpen [Identificatie](#), [authenticatie](#) en [autorisatie](#). Dit zijn essentiële ondersteunende functionaliteiten die nodig zijn om een [datadienst](#) tussen partijen ([datadienstaanbieder](#) en [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

i 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. Op dit moment is het afsprakenstelsel in ontwikkeling in het [DSGO-programma](#), in een toekomstige versie van het afsprakenstelsel zal deze worden uitgewerkt.



 **Generieke afspraken DSGO** 
Bijvoorbeeld: voor identificatie en authenticatie wordt gebruik gemaakt van erkende vertrouwensdienstverleners

 **Specifieke afspraken buiten DSGO**
Bijvoorbeeld: Bij projecten waar gevaarlijke chemische stoffen worden gebruikt, wordt de voortgang gedeeld met een centrale partij.

 **Specifieke afspraken DSGO** 
Bijvoorbeeld: dat een specifiek BIM IFC standaard wordt gebruikt bij het uitwisselen van BIM modellen.

 **Datadiensten**
Bijvoorbeeld: De voortgang van bouwprojecten wordt middels API's iedere 20 minuten ontsloten naar een centrale partij.

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


Generieke Afspraken

i In de [introdactie](#) 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.

- › [API Specifications](#)
- › [Generieke Technische Standaarden](#)
- › [Identificatie](#)
- › [Authenticatie](#)
- › [Autorisatie](#)
- › [Informatiebeveiliging](#)
- › [Juridische Context](#)
- › [Service Level Agreements](#)
- [Incidentenbeheer](#)
- [Marktvoorzieningen](#)

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 following API endpoints are specified:

- [Generic API Requirements](#)
- [API Service Content](#)
- [Data Service Resource](#)
- › [/subscriptions](#)
- › [/notifications](#)
- › [/token](#)

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.

:Q

uot **Source:** [iSHARE - Caching](#)

es:

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

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

Data Service Resource


 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.

```
1  [{
2    "id": "001",
3    "data": {
4      "colour": "red",
5      "value": "#f00",
6      "description": "Hex value of the colour red"
7    }
8  }, {
9    "id": "002",
10   "data": {
11     "colour": "green",
12     "value": "#0f0",
13     "description": "Hex value of the colour green"
14   }
15 }, {
16   ...
17 }]
```

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 their data service 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
class	Required	String representing the resource type, equal to subscription
href	Required	URL of the subscription, according to RFC3986
createdDateTime	Required	Date time when the subscription was initially created, according to ISO 8601
startDateTime	Required	Contains the date time when the subscription becomes/became valid, according to ISO 8601
endDateTime	Optional	If the subscription has an end date, or has ended, contains the end date and time, according to ISO 8601
consumerId	Required	If the subscription is assigned a data service consumer contains a unique identifier of the data service consumer as an EORI number
providerId	Required	Unique identifier of the data service provider as an EORI number
description	Optional	Description of the subscription
eventType	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
webhookUrl	Required	URL of the data service consumer that notifications shall be sent to, according to RFC3986

✓ Example of an subscription object


```
1 {
2   "id": "sub_123",
3   "class": "subscription",
4   "href": "/subscriptions/sub_123",
5   "createdDateTime": "2022-09-21T10:23:37Z",
6   "startDateTime": "2022-09-21T23:59:59Z",
7   "endDateTime": "2023-09-21T23:59:59Z",
8   "consumerId": "EU.EORI.NL000123456",
9   "providerId": "EU.EORI.NL000345678",
10  "description": "detailed description of the subscription",
11  "eventType": ["Modified", "Deleted"],
12  "status": "active",
13  "webhookUrl": "https://example.com/notifications"
14 }
```

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.

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

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](#)

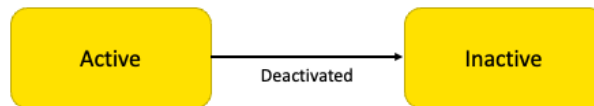
Visualize OpenAPI (Swagger) documentation app

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

Lifecycle of a Subscription

Within the [trust framework](#), [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.

i 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 subscription 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

Authentication

ⓘ This will be completed at a later date

Authorisation

ⓘ This will be completed at a later date

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

```
1 {
2   "count": 4,
3   "subscriptions": [
4     {
5       "id": "sub_123",
6       "class": "subscription",
7       "href": "/subscriptions/sub_123",
8       "createdDateTime": "2022-09-21T10:23:37Z",
9       "startDateTime": "2022-09-21T23:59:59Z",
```

```
10     "endTime": "2023-09-21T23:59:59Z",
11     "consumerId": "EU.EORI.NL000123456",
12     "providerId": "EU.EORI.NL000345678",
13     "description": "detailed description of the subscription",
14     "eventType": ["Modified"],
15     "status": "active",
16     "webhookUrl": "https://example.com/notifications"
17 },
18 {
19     "id": "sub_345",
20     "class": "subscription",
21     "href": "/subscriptions/sub_345",
22     "createdDateTime": null,
23     "startDateTime": null,
24     "endTime": null,
25     "consumerId": null,
26     "providerId": "EU.EORI.NL000345678",
27     "description": "detailed description of the subscription",
28     "eventType": ["Modified","Deleted"]
29     "status": "inactive",
30     "webhookUrl": null
31 },
32 {...},
33 {...},
34 ]
35 }
```

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

Authentication

ⓘ This will be completed at a later date

Authorisation

ⓘ This will be completed at a later date

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`
- `startDateTime` (optional)
- `endDateTime` (optional)
- `eventType`
- `webhookUrl`

✓ 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

```
1 {
2   "class": "subscription",
3   "createdDateTime": "2022-09-21T10:23:37Z",
4   "startDateTime": "2022-09-21T23:59:59Z",
5   "endDateTime": null,
6   "eventType": ["Modified"],
7   "webhookUrl": "https://example.com/notifications"
8 }
```

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 successful POST `/subscriptions` call

```
1 {
2   "id": "sub_123",
3   "class": "subscription",
4   "href": "/subscriptions/sub_123",
5   "createdDateTime": "2022-09-21T10:23:37Z",
6   "startDateTime": "2022-09-21T23:59:59Z",
7   "endDateTime": "2023-09-21T23:59:59Z",
8   "consumerId": "EU.EORI.NL000123456",
9   "providerId": "EU.EORI.NL000345678",
10  "description": "detailed description of the subscription",
11  "eventType": ["Modified"],
12  "status": "active",
13  "webhookUrl": "https://example.com/notifications"
14 }
```

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

Authentication

- ⓘ This will be completed at a later date

Authorisation

- ⓘ This will be completed at a later date

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

```
1 {
2   "id": "sub_123",
3   "class": "subscription",
4   "href": "/subscriptions/sub_123",
5   "createdDateTime": "2022-09-21T10:23:37Z",
6   "startDateTime": "2022-09-21T23:59:59Z",
```

```
7  "endTime": "2023-09-21T23:59:59Z",
8  "consumerId": "EU.EORI.NL000123456",
9  "providerId": "EU.EORI.NL000345678",
10 "description": "detailed description of the subscription",
11 "eventType": ["Modified"],
12 "status": "active",
13 "webhookUrl": "https://example.com/notifications"
14 }
```

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

Authentication

- ⓘ This will be completed at a later date

Authorisation

- ⓘ This will be completed at a later date

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

Authentication

- ⓘ This will be completed at a later date

Authorisation

- ⓘ This will be completed at a later date

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

/notifications

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

In order for a [data service consumer](#) to [subscribe](#) to a [data service](#), 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
<code>id</code>	Required	Unique identifier of the subscription
<code>class</code>	Required	String representing the object type, equal to <code>notification</code>
<code>dateTime</code>	Required	Date and time that the notification was sent, according to ISO 8601
<code>consumerId</code>	Required	Unique identifier of the data service consumer as an EORI number
<code>providerId</code>	Required	Unique identifier of the data service provider as an EORI number
<code>subscriptionId</code>	Required	Unique identifier of the subscription under which the event is monitored
<code>description</code>	Optional	Description of the notification
<code>event</code>	Required	event object, as defined here , containing data regarding the event which triggered the notification

Example notification object

```
1 {
2   "id" : "not_123",
3   "class" : "notification",
4   "dateTime" : "2022-09-21T10:23:48Z",
5   "consumerId" : "EU.EORI.NL000123456",
6   "providerId" : "EU.EORI.NL000345678",
7   "subscriptionId" : "sub_123",
8   "description" : "Detailed description of the notification",
9   "event" : [
10    {
11      "id" : "eve_123",
12      "objectType" : "event",
13      "eventType" : "Modified",
14      "dateTime" : "2022-09-21T10:23:37Z",
15      "description" : "Detailed description of the event",
16      "eventData" : "Data record xyz has been modified by zyx"
```

```
17     }
18   ]
19 }
```

Event object

Parameters		Description
id	Required	Unique identifier of the event
class	Required	String representing the object type, equal to event
eventType	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
dateTime	Required	Date and time that the event took place, according to ISO 8601
description	Optional	Detailed description of the event
eventData	Optional	Optional data related to the event

Example of an event object

```
1 {
2   "id" : "eve_123",
3   "class" : "event",
4   "eventType" : "Modified",
5   "dateTime" : "2022-09-21T10:23:37Z",
6   "description" : "Detailed description of the event",
7   "eventData" : "Data record xyz has been modified by zyx"
8 }
```

Endpoint

The notification endpoint allows data service consumers to receive and act upon notifications from a data service provider.

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

Authentication

- ⓘ This will be completed at a later date

Authorisation

- ⓘ This will be completed at a later date

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

```
1 {
2   "id" : "not_123",
3   "object" : "notification",
4   "dateTime" : "2022-09-21T10:23:48Z",
5   "consumerId" : "EU.EORI.NL000123456",
6   "providerId" : "EU.EORI.NL000345678",
7   "subscriptionId" : "sub_123",
8   "description" : "Detailed description of the notification",
9   "event" : [
10    {
11      "id" : "eve_123",
12      "objectType" : "event",
13      "eventType" : "Modified",
14      "dateTime" : "2022-09-21T10:23:37Z",
15      "description" : "Detailed description of the event",
16      "eventData" : "Data record xyz has been modified by zyx"
17    }
18  ]
19 }
```

Responses

Authentication

 This will be completed at a later date

Due to possible non-repudiation requirements for notifications, responses to notifications may require authentication


Authorisation

 This will be completed at a later date


Due to possible non-repudiation requirements for notifications, responses to notifications may require 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

/token

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

Access tokens are used by [data service consumers](#) as credentials to gain access to a [data service](#). Access tokens can be requested at a [data services provider](#) via the `/token` endpoint. See the [M2M Authentication Flow](#) page for more information about how this endpoint can be used.

 Data service providers MUST provide an access token via 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](#) for a [data service consumer](#) at a [data service provider](#). This method results in an access token with which the data service consumer can gain access to a [data service](#). The format of an access token is not defined by this specification. They are left to the server and should be opaque to a data service consumer.

✓ Data service providers MUST support a POST call to a `/token` endpoint to create a new access token

Request

Headers

✓ Data service providers MUST validate that a POST request to a `/token` endpoint contains the HTTP headers as described in the table below

Header		Description
<code>Content-Type</code>	Required	as the OAuth 2.0 JWT bearer profile, specified in RFC7523 . Defines request body content type. Must be equal to <code>application/x-www-form-urlencoded</code>

Parameters

For information about the parameters that are common to [trust framework's](#) API's see [Generic API Requirements](#).

✓ Data service providers MUST validate that a POST request to a `/token` endpoint contains the parameters as described in the table below

✓ Data service providers MUST validate the client credentials in the `client_assertion` received in a POST to a `/token` endpoint

Parameters		Description
<code>grant_type</code>	Required	as the OAuth 2.0 grant type. MUST be equal to <code>client_credentials</code>
<code>scope</code>	Required	as the OAuth 2.0 scope. MUST contain the value <code>dsgo</code>
<code>client_id</code>	Required	as the OAuth 2.0 JWT bearer profile, specified in RFC7523 . Used in DSGO for client identification. MUST contain a valid EORI identifier of the data service consumer. (see Identificatie van Organisaties)
<code>client_assertion_type</code>	Required	as the OAuth 2.0 JWT bearer profile, specified in RFC7523 . MUST be equal to <code>urn:ietf:params:oauth:client-assertion-type:jwt-bearer</code>
<code>client_assertion</code>	Required	as the OAuth 2.0 JWT bearer profile, specified in RFC7523 . Used in DSGO for authentication of the client identification. MUST contain a signed JWT

Example request body for a POST /token call

```
1 {
2   "grant_type"="client_credentials"&
3   "scope"="dsgo"&
4   "client_id"="EU.EORI.NL000000001"&
5   "client_assertion_type"="urn:ietf:params:oauth:client-assertion-type:jwt-bearer"&
6   "client_assertion"="eyJhbGciOiJSUzI1NiIsImtpZCI6IjYIn0.eyJpc3Mi[...]cC4hiUpo[...]o
7 }
```

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

✓ Data service providers MUST include the HTTP headers as described in the table below in a response to a POST request to a `/token` endpoint

Header	Required	Description
<code>content-Type</code>	Required	Defines response body content type. Must be equal to "application/json"

Payload

✓ Data service providers 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

Parameters	Required	Description
<code>access_token</code>	Required	as the OAuth 2.0 access token. The access token which will be used to access endpoints that require authorization
<code>token_type</code>	Required	as the OAuth 2.0 JWT bearer profile, specified in RFC7523 . MUST be equal to "bearer"
<code>expires_in</code>	Required	Access token expiration time in seconds. SHOULD be "3600"
<code>refresh_token</code>	Optional	as the OAuth 2.0 refresh token, which can be used to obtain new access tokens using the same authorization grant

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

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

```
1 {
2   "access_token": "aW2ys9NGE8RjHPZ4mytQivkWJ05HGQCYJ7VvMNGDLI0w",
3   "token_type": "bearer",
```

```
4   "expires_in":3600
5 }
```

400 Bad Request

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

- ✓ Data service providers 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
<code>error</code>	Required	as specified in OAuth 2.0 section 5.2 , an error code
<code>error_description</code>	Optional	as specified in OAuth 2.0 section 5.2 , a human-readable text providing additional information
<code>error_uri</code>	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

```
1 {
2   "error":"invalid_request"
3 }
```

POST /token/revoke

Revokes an [access token](#) previously obtained. This method results in the revocation of an access token by a [data service provider](#) such that it cannot be used by the [data service consumer](#) to gain access to a [data service](#).

✓ Data service providers MUST support a POST call to a `/token/revoke` endpoint to revoke an access token

Request

Headers

✓ Data service providers MUST validate that a POST request to a `/token/revoke` endpoint contains the HTTP headers as described in the table below

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

Parameters

For information about the parameters that are common to [trust framework's](#) API's see [Generic API Requirements](#).

✓ Data service providers MUST validate that a POST request to a `/token/revoke` endpoint contains the parameters as described in the table below

✓ Data service providers MUST validate the client credentials in the `client_assertion` received in a POST to a `/token/revoke` endpoint

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

token	Required	as the OAuth 2.0 access token. MUST be equal to access token that the client wants revoked as specified in RFC7009
<div style="border: 1px solid #ccc; padding: 5px;"> <p>Example request body for a POST /token/revoke call</p> <pre> 1 { 2 "grant_type"="client_credentials" 3 "client_id"="EU.EORI.NL000000001"& 4 "client_assertion_type"="urn:ietf:params:oauth:client-assertion-type:jwt-bearer"& 5 "client_assertion"="eyJhbGciOiJIUzI1NiIsImtpZCI6IjIyIn0.eyJpc3MiOiI...omitted for brevity...".cC4hiUPo[...o 6 "token"="aW2ys9NGE8RjHPZ4mytQivkWJ05HGQCYJ7VyMNGDLI0w" 7 }</pre> </div>		

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.

- ✓ Data service providers MUST respond with a `200 OK` to a successful POST call to a `/token/revoke` endpoint
- ✓ Data service providers MUST respond with a `200 OK` to a POST call to a `/token/revoke` endpoint containing an invalid access token
- ✓ Data service providers MUST no longer accept the revoked the acces token after a `200 OK` response is responded

400 Bad Request

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

- ✓ Data service providers 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.

<div style="border: 1px solid #ccc; padding: 5px;"> <p>Example HTTP payload in a response to a failed POST to the /token/revoke endpoint</p> <pre> 1 { 2 "error": "invalid_request" 3 }</pre> </div>		
--	--	--

503 Service Unavailable

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

- ✓ Data service consumers MAY include a `Retry-After` header in the 503 response to indicate the expected unavailability of the service

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 web servers. 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 web servers. 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 gebruikt 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 ZOUDE RESTful architectuurprincipes MOETEN volgen voor API's

Introductie API's

:Q

uot **Bron:** API strategie voor de Nederlandse Overheid - [2.3 Wat is een API](#)

es:

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](#).

:Q

uot **Bron:** API strategie voor de Nederlandse Overheid - [4.2 RESTful principes](#)

es:

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
<code>POST</code>	Create	Wordt gebruikt als een "create" voor resources (ofwel <code>POST</code> 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

:Q

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

es:

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 protocol

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.

:Q
uot Bron: iSHARE - HTTP(s)
es:
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 authenticatievenster 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 precondition 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)

:Q

uot **Bron:** API strategie voor de Nederlandse Overheid - [HTTP statuscodes](#)

es:

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 <code>Location</code> 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 ZOULDEN 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 communiceren in UTC-tijd

✓ Partijen MOETEN alle datums en tijdstippen vastgelegd in de generieke technische standaarden formatteren volgens het UNIX timestamp format

Identificatie

Identificatie is in het kader van DSGVO 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 geïnteracteed 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](#).

- 📌 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 attributsets 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 uitwisselen 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 DSGVO 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 DSGVO 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

i 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

i **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 juiste [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](#) gebeurt niet op transport niveau, maar op datadienst niveau via een getekende JWS

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.

:Q

uot **Bron:** eHerkenning – [Betrouwbaarheidsniveaus](#)

es:

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 eHerkenningmiddel
- 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 mate 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 vermindert en gebruikers ervaring versimpeld omdat het om minder gevoelige data gaat.

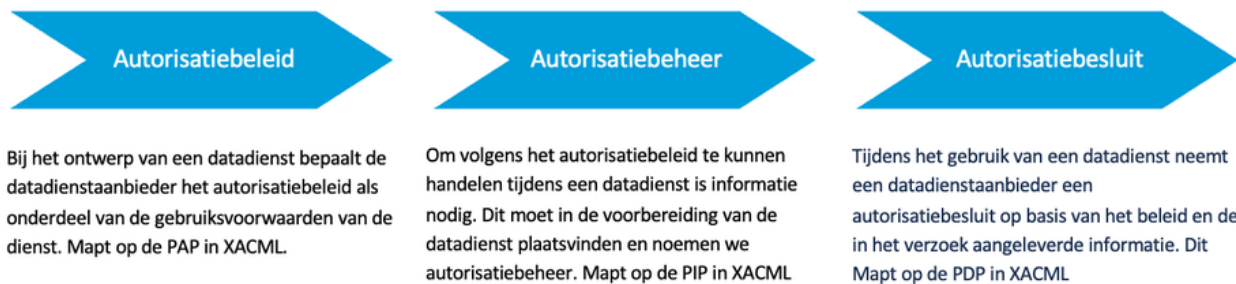
Elementen die van belang zijn bij het onderwerp van betrouwbaarheidsniveaus zijn bijvoorbeeld:

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

ⓘ 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 draait autorisatie om het vaststellen of de geïdentificeerde de rechten heeft en toestemming krijgt om een specifieke actie uit te voeren gegeven de context van de datadienst. In het [afsprakenstelsel](#) is het onderwerp van autorisatie gesplitst in [autorisatiebeleid](#), [autorisatiebeheer](#), en [autorisatiebesluit](#) (zie figuur hieronder). De uitwerking van deze onderdelen is gebaseerd op de XACML standaard voor (online) autorisatie/toegangsbeleid. Gegeven XACML, mapt het autorisatiebeleid op PAP, autorisatiebeheer op het organiseren van PIP en het autorisatiebesluit op PDP. De 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

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

- ° [Autorisatiebeleid](#)
- ° [Autorisatiebeheer](#)
- > [Autorisatiebesluit](#)

Autorisatiebeleid

Het [autorisatiebeleid](#) is specifiek voor een [datadienst](#) en beschrijft de gebruiksvoorwaarde en toegangscontroleregels waaraan moet worden voldaan om de dienst af te mogen nemen. Daarbinnen ligt vast wie [rechthebbende](#) 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 [datadienstdefinitie](#) zal de informatie over het autorisatiebeleid bevatten.

 Merk op: de gedetailleerde eisen rondom autorisatiebeleid worden in een toekomstige versie van het afsprakenstelsel uitgewerkt.

Autorisatiebeheer

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 [autorisatiebeheer](#) worden de voorbereidingen getroffen om deze informatie beschikbaar te stellen bij het maken van het autorisatiebesluit. Afhankelijk van het autorisatiebeleid kan het autorisatiebeheer over verschillende type informatie gaan. Bijvoorbeeld het uitgeven van bepaalde kwalificaties en eigenschappen die bij het datadienstverzoek nodig zijn of het registreren van [gedelegeerde](#) rechten.


Kwalificaties en eigenschappen

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.

Delegatie

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 delegaties kunnen worden geregistreerd zodat deze als informatie kunnen worden gebruikt door de datadienstaanbieder bij het maken een autorisatiebesluit.

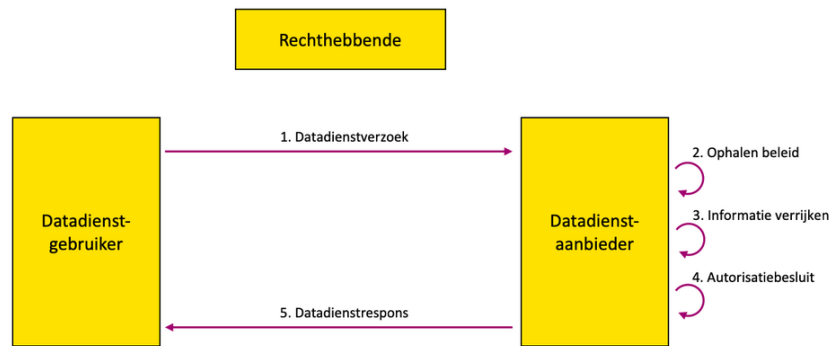
- 1. De rechthebbende beheert zelf delegaties** De rechthebbende heeft (in afstemming met de datadienstaanbieder) bepaald dat de rechthebbende voor elk verzoek om een datadienst toestemming moet geven. De rechthebbende stelt hiervoor de eisen op en zorgt voor een operationeel proces dat het mogelijk maakt dit uit te voeren en als informatie aan te leveren aan de datadienstaanbieder bij een datadienstverzoek. Dit is geschikt voor datadiensten met zeer waardevolle data waar de rechthebbende volledige controle over wil hebben.
- 2. De rechthebbende registreert zijn delegaties bij de datadienstaanbieder** De rechthebbende heeft instructies/regels/beleid bepaald op basis waarvan de datadienstaanbieder autonoom autorisatiebesluiten kan nemen. Het datadienstverzoek zal informatie bevatten over de datadienstgebruiker op basis waarvan de datadienstaanbieder in staat is om deze zelfstandig te controleren tegen het autorisatiebeleid. Dit is geschikt wanneer de datadienstaanbieder over de software beschikt welke technische integratie mogelijk maakt tussen de rechthebbende en de datadienstaanbieder.
- 3. De rechthebbende registreert zijn delegaties bij een onafhankelijk [autorisatieregister](#).** De rechthebbende heeft voordat een datadienstverzoek plaatsvindt zijn delegaties geregistreerd in een autorisatieregister. Vervolgens, wanneer de datadienstaanbieder een datadienstverzoek ontvangt, wordt het autorisatieregister bevraagd of de datadienstgebruiker de nodige rechten heeft. Dit is geschikt wanneer schaalbaarheid belangrijk is. Een autorisatieregister kan het beheer van een groot aantal delegaties op zich nemen.

 Merk op, nog niet alle autorisatiebeheer mogelijkheden zijn in detail uitgewerkt. In de toekomstige versie van het afsprakenstelsel zal dit verder worden gedetailleerd.

Autorisatiebesluit

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 het autorisatiebeleid en de informatie die nodig is.

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



Interactiemodel om tot een autorisatiebesluit te komen

#	Acties	Omschrijving
1	Datadienst verzoek	De datadienstgebruiker dient een verzoek tot het gebruik van een datadienst in bij de datadienstaanbieder.
2	Ophalen beleid	De datadienstaanbieder haalt het autorisatiebeleid op van de datadienst .
3	Informatie verrijken	De datadienstaanbieder haalt eventueel extra informatie op die nodig is bij het komen tot een autorisatiebesluit.
4	Autorisatiebesluit	De datadienstaanbieder komt op basis van het autorisatiebeleid en de beschikbare informatie tot een autorisatiebesluit.
5	Uitvoeren besluit	De datadienstaanbieder voert het resultaat van het autorisatiebesluit uit (geeft al dan niet toegang).

Om tot een autorisatiebesluit te komen zijn verschillende mechanismes nodig, afhankelijk van de situatie die geldt voor die specifieke datadienst. In het afsprakenstelsel zijn aparte mechanismes gedefinieerd voor grofmazige en fijnmazige autorisaties voor beide **machine-to-machine** en **human-to-machine** interacties.

> [Grofmazig en fijnmazige autorisatie](#)

i Op dit moment is het afsprakenstelsel in ontwikkeling, in een toekomstige versie van het afsprakenstelsel zal deze onderwerpen worden gedetailleerd.

Grofmazig en fijnmazige autorisatie

Om een breed scala aan [datadiensten](#) mogelijk te maken wordt in het [afsprakenstelsel](#) verschillende mechanisme gedefinieerd voor grofmazige en fijnmazige [autorisaties](#). Grofmazige autorisatie wordt gedaan op basis van een geauthenticeerde identiteit van de juridische entiteit van de [datadienstgebruiker](#). Voor sommige datadiensten zal grofmazige autorisatie voldoende zijn voor het nemen van [autorisatiebesluit](#). Indien nodig kan na grofmazige autorisatie de datadienstgebruiker fijnmazig worden geautoriseerd voor het gebruik van de datadienst.

★ **Indicatieve voorbeelden:**

Grofmazige autorisatie: Voor een datadienst waar de locatie van warmtepompinstallaties in een gebouw wordt gedeeld van een beheerder (datadienstaanbieder) met een installateur (datadienstgebruiker) is grofmazige autorisatie voldoende omdat de locaties gezien mogen worden door elke gebruiker van die juridische entiteit van de installateur.

Fijnmazige autorisatie: Voor een datadienst waar gevoelige contractdata wordt gedeeld van een opdrachtgever (datadienstaanbieder) met een aannemer (datadienstgebruiker) is grofmazige autorisatie onvoldoende omdat de contractdata enkel beschikbaar moet worden gesteld aan de juiste verantwoordelijke account manager van de aannemer. In dit geval zal fijnmazige autorisatie nodig zijn bovenop de grofmazige autorisatie

Op de onderliggende pagina's worden deze onderwerpen verder gedetailleerd:

* [Grofmazig M2M Autorisatie Flow](#)

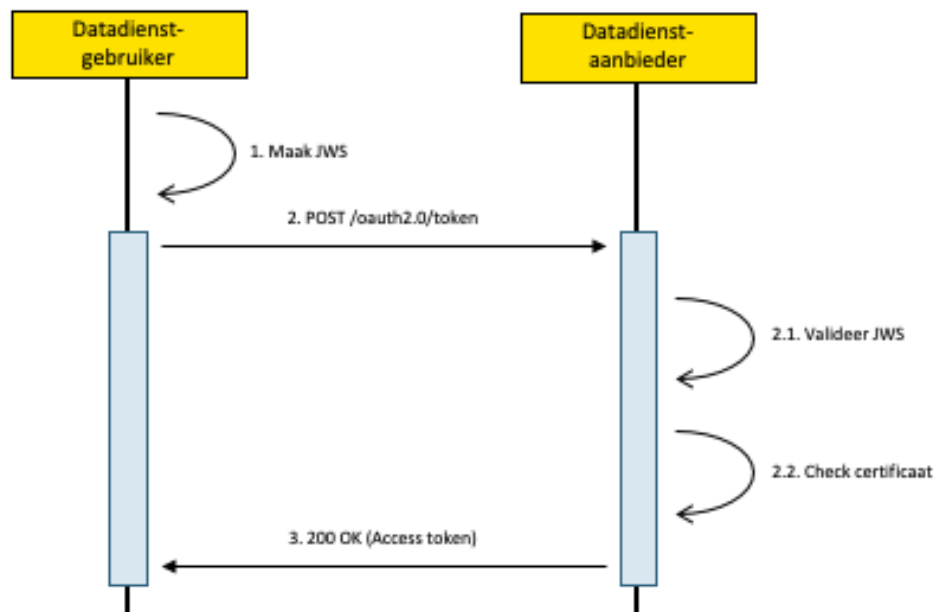
i Op dit moment is het afsprakenstelsel in ontwikkeling, in een toekomstige versie van het afsprakenstelsel zal dit onderwerp worden gedetailleerd.

Grofmazig M2M Autorisatie Flow

Bij het aanbieden van [datadiensten](#) is [autorisatie](#) een essentieel onderdeel. Een (potentiele) [datadienstgebruiker](#) moet aan tonen dat ze geautoriseerd zijn om gebruik te maken van een datadienst van een [datadienstaanbieder](#). Voor grofmazige autorisatie (op basis van de een [authenticeerde identiteit](#) van de datadienstgebruiker) wordt in het [afsprakenstelsel](#) [access tokens](#) gebruikt. Een access token dienst als bewijs dat de datadienstgebruiker geauthenticeerd is en de rechten heeft om een datadienstverzoek te sturen. Indien nodig, kan fijnmazige autorisatie specifiek voor de datadienst worden gedaan wanneer een datadienstverzoek wordt gedaan met het access token.

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 [identificatie](#) van de datadienstgebruiker geauthenticeerd. Hiervoor wordt een [JWS](#) gebruikt volgens de [OAuth 2.0 JWT bearer profile](#). In de onderstaande figuur worden de stappen weergegeven waarin een datadienstgebruiker een access token kan aanvragen bij de datadienstaanbieder.

Merkp op, Deze flow wijkt op dit moment af van die beschreven in iSHARE (zie [link](#)). Dit is omdat er in het DSGO nog geen keuze is gemaakt over de invulling van de "scheme owner" rol. Wanneer deze keuze wordt gemaakt kan deze flow worden aangevuld.



Overzicht van de grofmazige M2M autorisatie flow

1. Maak JWS

De datadienstgebruiker maakt een JWS om mee te sturen in het verzoek voor een access token. Deze JWS dient alle benodigde informatie te bevatten op basis waarvan de datadienstaanbieder de datadienstgebruiker kan identificeren en authenticeren en op basis daarvan een grofmazige autorisatie bepalen.

✓ Datadienstgebruikers MOETEN een JWS maken volgens de [JWS specificaties](#)

2. POST /oauth2.0/token

In deze handeling dient de datadienstgebruiker een verzoek in bij de datadienstaanbieder tot het verstrekken van een access token. De aanvraag van de datadienstgebruiker bevat de JWS gemaakt in de vorige stap. De details van deze API request zijn verder gedetailleerd

op de [POST /token](#) pagina.

2.1. Valideer JWS

De datadienstaanbieder valideert of de aanvraag een geldige [JWS](#) bevat.

✓ Datadienstaanbieders MOETEN de JWS valideren volgens de [JWS specificaties](#)

2.2. Check certificaat

In deze handeling controleert de datadienstaanbieder het certificaat waarmee de JWS is getekend. Meer details over deze informatie is te vinden op de [ondertekening](#) pagina

3. 200 OK (Access token)

Wanneer de vorige stappen succesvol zijn uitgevoerd door de datadienstaanbieder kan deze de grofmazige [autorisatiebesluit](#) nemen op basis van de geauthenticeerde identiteit van de datadienstgebruiker. Indien succesvol, wordt een access token terug gestuurd naar de datadienstgebruiker. De details van deze API response zijn verder gedetailleerd op de [POST /token](#) pagina.

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 \(JWT\)](#)

 **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 ZOULDEN een risicoanalyse uit MOETEN voeren

✓ Partijen ZOULDEN passende informatiebeveiligingsmaatregelen MOETEN nemen

✓ Partijen ZOULDEN 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 (HyperText 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.

:Q

uot **Bron:** API strategie voor de Nederlandse Overheid - [API Beveiliging](#)

es:

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 ZOULDEN 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 webserver 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).

:Q

uot **Bron:** European Parlaimant - [Qualified certificates for website authentication](#)

es:

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. Verder wordt additionele informatie meegestuurd zoals beschreven in [ETSI TS 119 182-1](#) om de onweerlegbaarheid content waar in de JWT naar wordt verwezen te garanderen.

Op deze pagina worden de generieke afspraken die gelden voor het gebruik van JWS 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.

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 JWTs ondertekenen als een JSON Web Signature (JWS) zoals beschreven in [RFC 7515](#)

✓ Partijen MOETEN JWS formateren volgens JWS Compact Serialisation

JWS Header

✓ Partijen MOETEN het RS256 algoritme gebruiken bij het ondertekenen van een JWS

✓ Partijen MOETEN in JWS headers de parameters gebruiken zoals opgesteld in de onderstaande tabel. Partijen MOGEN andere parameters NIET gebruiken

JWS header fields		Beschrijving
alg	VEREIST	Als beschreven in RFC 7515 , MOET ingevuld worden als <code>"RS256"</code>
b64	VEREIST	Als beschreven in RFC 7797 , MOET ingevuld worden als <code>false</code>
crit	VEREIST	Als beschreven in RFC 7515 , MOET ingevuld worden als <code>["sigT", "sigD", "b64"]</code>
sigT	VEREIST	Als beschreven in ETSI TS 119 182-1 , MOET ingevuld worden als het tijdstip dat de tekening is gezet, geformatteerd volgens UTC
sigD	VEREIST	Als beschreven in ETSI TS 119 182-1 , MOET ingevuld worden met <code>"mId"</code> gelijk aan <code>"http://uri.etsi.org/19182/HttpHeaders"</code> en <code>"pars"</code> MOET de volgende volgende HTTP Header fields bevatten: <ul style="list-style-type: none"><code>"(request-target)"</code> (voor HTTP Requests),<code>"host"</code> (als aanwezig),<code>"content-type"</code> (als aanwezig),<code>"content-encoding"</code> (als aanwezig),

		<ul style="list-style-type: none"> • "digest" (als aanwezig)
typ	VEREIST	MOET ingevuld worden als "JOSE"
x5c	VEREIST	Als beschreven in RFC7523, zal de QSEAL voor de ondertekening bevatten

De sigT header is toegevoegd 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 om een handtekening over specifieke HTTP headers en de HTTP body te kunnen zetten om deze te beveiligen.

Een JWS header ziet er bijvoorbeeld uit zoals hieronder:

```

  ✓ Voorbeeld JWS header
  1 {
  2   "alg": "RS256",
  3   "b64": false,
  4   "crit":[
  5     "sigT",
  6     "sigD",
  7     "b64"
  8   ],
  9   "sigT":"2020-10-26T11:26:57Z",
 10  "sigD":{
 11    "pars":[
 12      "(request-target)",
 13      "host",
 14      "content-type",
 15      "content-encoding",
 16      "digest"
 17    ],
 18    "mId":"http://uri.etsi.org/19182/HttpHeaders"
 19  },
 20  "typ": "JOSE",
 21  "x5c":[
 22    "MIIGCDCCA/CgAwIBAgICEAQwDQYJKoZIhvcNAQELBQAwwZAxChAJBgNVBAYTAk5MMQswCQYDVQQIDAJOSDEPMA0GA1UECgwGaVNIQVJ
 23    "MIIGBDCCA+ygAwIBAgICEAAwDQYJKoZIhvcNAQELBQAwwZAxChAJBgNVBAYTAk5MMQswCQYDVQQIDAJOSDESMBAGA1UEBwwJQW1zdGV
 24    "MIIGCDCCA/CgAwIBAgIJAN7kMSjuGT9KMA0GCSqGSIb3DQEBCwUAMIGQMswCQYDVQQGEWJOTDELMAkGA1UECAwCTkgxEjAQBgnVBAC
 25  ]
 26 }

```

JWS Payload

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

- ✓ Partijen MOETEN een JWS payload "detached" maken van de handtekening, zoals beschreven in RFC 7515 Appendix F
- ✓ Partijen MOETEN JWS claims opstellen volgens het "JWT Bearer profile" als beschreven in RFC 7523
- ✓ Partijen MOETEN in JWS claims de parameters gebruiken zoals opgesteld in de onderstaande tabel
- ✓ Partijen ZOUDENIET andere JWS claims MOETEN definiëren en gebruiken, afhankelijk van het specifieke gebruik van de JWS

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 JWS claims toe te voegen. Datadienst specifieke claims zouden in de resource moeten worden meegenomen

✓ Partijen MOETEN JWS claims binnen 30 seconden laten verlopen, aantoonbaar door de combinatie van `iat` en `exp` claims.

✓ Partijen MOETEN zowel `iat` als `exp` claims noteren in seconden en MOGEN `iat` en `exp` claims NIET noteren in milliseconden

Een JWS payload ziet er bijvoorbeeld uit zoals hieronder (Bron: iSHARE - JSON Web Token)

▼ Voorbeeld JWS payload

```

1 {
2   "iss": "EU.EORI.NL123456789",
3   "sub": "EU.EORI.NL123456789",
4   "aud": "EU.EORI.NL987654321",
5   "jti": "378a47c4-2822-4ca5-a49a-7e5a1cc7ea59",
6   "exp": 1504683475,
7   "iat": 1504683445
8 }
```

JWS Verwerking

✓ Partijen MOETEN een JWS maar één keer accepteren

✓ Partijen MOETEN een JWS 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 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 [JWS](#) om de integriteit en onweerlegbaarheid van interacties tussen partijen waar te borgen. Het tekenen van JWS 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 API requests

✓ Partijen MOETEN alle root certificaten voor QSEALS van CAs op de EU/EEA [List of Trusted Lists](#) (LOTL) en [PKIO](#) accepteren

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.

:Q

uot **Bron:** Europese Commissie - [Wat zijn persoonsgegevens?](#)

es:

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

:Q

uot **Bron:** Autoriteit Persoonsgegevens - [Belangrijkste bepalingen AVG](#)

es:

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.

:Q

uot **Bron:** Autoriteit Persoonsgegevens - [Mag ik uw persoonsgegevens verwerken?](#)

es:

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 afsprakenstelsels 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 DSGVO 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 overgangperiode 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 speelveld te creëren 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 dat SLAs over beschikbaarheid geen rekening houdt met incidenten (zie [Incidenten](#) voor deze eisen).

✓ 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

! **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 ZOUDE ten minste 100 API verzoeken moeten kunnen verwerken binnen het beschikbaarheidsvenster

Incidenten

Een incident is een gebeurtenis die niet tot de standaardoperatie van een datadienst behoort en mogelijk leidt tot het verlies van vertrouwen, veiligheid en integriteit van het afsprakenstelsel, net als datadiensten die erop zijn geïmplementeerd. Wanneer een incident wordt gemeld door een datadienstgebruiker, gelden de volgende eisen. Zie het [Incidentbeheer](#) voor de informatie over de melding van incidenten, de classificatie van incidenten (prioriteiten) en het incidentafhandelingsproces.

Het oplossen van incidenten maakt geen deel uit van regulier onderhoud, en valt niet onder de beschikbaarheidsvensters zoals beschreven.

- ✓ Datadienstaanbieders MOETEN voor alle Prioriteit 1 en Prioriteit 2 incidenten een incident manager beschikbaar stellen

- ✓ Datadienstaanbieders ZOUDE voor alle Prioriteit 1 en Prioriteit 2 incidenten een incident manager 24u per dag, 7 dagen per week beschikbaar MOETEN stellen

- ✓ Datadienstaanbieders MOETEN voor een Prioriteit 1 incident een update delen met de beheerorganisatie binnen 2 uur van elke belangrijke update en elke 4 uur

- ✓ Datadienstaanbieders MOETEN voor een Prioriteit 2 incident een update delen met de beheerorganisatie binnen 2 uur van elke belangrijke update aan het einde van elke werkdag

- ✓ Datadienstaanbieders MOETEN voor een Prioriteit 3 incident een volledige update delen met de beheerorganisatie aan het einde van elke werkdag

- ⓘ Merk op, het gedetailleerde incident afhandelingsprocedure zal als apart hoofdstuk verder worden gedetailleerd als operationeel proces. Deze wordt op een later moment uitgewerkt.

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 ZOUDE op een passende frequentie een back-up MOETEN maken van data belangrijk voor de datadienst

- ✓ Datadienstaanbieders ZOUDE 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 ZOUDE bereikbaar MOETEN zijn voor ondersteuning via e-mail

- ✓ Datadienstaanbieders ZOUDE binnen een werkdag na ontvangst van een vraag, verzoek of klacht MOETEN aangeven dat hiervan kennis is genomen

- ✓ Datadienstaanbieders ZOULDEN 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

- ⓘ 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.

Incidentenbeheer

Een incident is een gebeurtenis die niet tot de standaardoperatie van een [datadienst](#) behoort en mogelijk leidt tot het verlies van vertrouwen, veiligheid en integriteit van het [afsprakenstelsel](#), net als datadiensten die erop zijn geïmplementeerd.

Incidenten melden

✓ Partijen MOETEN incidenten direct na ontdekking melden bij de beheerorganisatie

ⓘ Het proces voor het melden van incidenten wordt in een volgende versie van het afsprakenstelsel gedetailleerd.

Incidentafhandelingsproces

ⓘ Het Incidentafhandelingsproces wordt in een volgende versie van het afsprakenstelsel gedetailleerd.

Incidenten classificatie

Een storing in de standaard operatie van een [datadienst](#) wordt in het [afsprakenstelsel](#) gemeld als een incident. Drie soorten incidenten zijn geclassificeerd afhankelijk van de geschatte impact volgens het onderstaande framework. Wanneer een incident aan minimaal een van de karakteristieken voldoet, wordt het incident op minimaal dat niveau geclassificeerd. Deze incidenten classificatie is gebaseerd op die gebruikt in [iSHARE](#).

Classificatie	Mogelijke Karakteristieken
Prioriteit 3 - Laag	<ul style="list-style-type: none">• Verwachte duur van minder dan 4 uur binnen het beschikbaarheidsvenster• Betrokkenheid van 1 partij• (Mogelijke) datalek, bijvoorbeeld door het verlies van een harde schijf, of door malware• Fraude of het vermoeden van fraude, bijvoorbeeld door een werknemer of hacker
Prioriteit 2 - Midden	<ul style="list-style-type: none">• Verwachte duur van meer dan 4 uur binnen het beschikbaarheidsvenster• Betrokkenheid van minimaal 5 partijen• Datalek met meldplicht bij de Autoriteit Persoonsgegevens• Impact op vertrouwelijkheid en integriteit.
Prioriteit 1 - Hoog	<ul style="list-style-type: none">• Verwachte duur van meer dan 12 uur binnen het beschikbaarheidsvenster• Betrokkenheid van minimaal 10 partijen• Grote impact op imago en vertrouwen van het DSGO• Politieke implicaties• Fundamentele juridische of technische kwetsbaarheid.

✓ Datadienstaanbieders MOETEN de datum, tijd en ingeschatte incident classificatie, en impact op de datadienst melden bij de rapportage over een incident

✓ De beheerorganisatie MOET het incident beoordelen en legt het classificatie niveau vast

✓ Datadienstaanbieders MOETEN handelen volgens de SLAs bijhorende bij de vastgestelde classificatie van het incident

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 Authorization Registry volgens iSHARE

Specifieke Afspraken

In dit hoofdstuk worden de specifieke afspraken die van toepassing zijn op [datadiensten](#) gepresenteerd.

- In de [introdactie](#) 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](#), en zijn nog geen specifieke afspraken uitgewerkt. In een toekomstige versie van het afsprakenstelsel zal deze worden ontwikkeld in dit hoofdstuk.

Appendix

De appendix bevat extra informatie en context waar in het afsprakenstelsel aan wordt gerefereerd.

- [Overzicht van Eisen](#)
- [Begrippenlijst \(Glossary\)](#)
- [FAQ](#)

Overzicht van Eisen

Voor een overzicht van de notatieconventies gebruikt in de eisen zie [deze pagina](#). Dit overzicht van eisen is ook beschikbaar als een excel sheet, [klik hier](#) om deze te downloaden.

Generieke Afspraken

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

API Service Content

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

Data Service Resource

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

/subscriptions

- ✓ Data service providers MUST define subscriptions for their data service 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

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`
 - `startDateTime` (optional)
 - `endDateTime` (optional)
 - `eventType`
 - `webhookUrl`
- ✓ 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

/notifications

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

✓ Data service consumers MUST support a notification object

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

/token

✓ Data service providers MUST provide an access token via the `/token` endpoint

POST /token

✓ Data service providers MUST support a POST call to a `/token` endpoint to create a new access token

✓ Data service providers MUST validate that a POST request to a `/token` endpoint contains the HTTP headers as described in the table below

✓ Data service providers MUST validate that a POST request to a `/token` endpoint contains the parameters as described in the table below

✓ Data service providers MUST validate the client credentials in the `client_assertion` received in a POST to a `/token` endpoint

✓ Data service providers MUST include the HTTP headers as described in the table below in a response to a POST request to a `/token` endpoint

✓ Data service providers 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

✓ Data service providers 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`

✓ Data service providers MUST support a POST call to a `/token/revoke` endpoint to revoke an access token

✓ Data service providers MUST validate that a POST request to a `/token/revoke` endpoint contains the HTTP headers as described in the table below

✓ Data service providers MUST validate that a POST request to a `/token/revoke` endpoint contains the parameters as described in the table below

✓ Data service providers MUST validate the client credentials in the `client_assertion` received in a POST to a `/token/revoke` endpoint

✓ Data service providers MUST respond with a `200 OK` to a successful POST call to a `/token/revoke` endpoint

✓ Data service providers MUST respond with a `200 OK` to a POST call to a `/token/revoke` endpoint containing an invalid access token

✓ Data service providers MUST no longer accept the revoked the acces token after a `200 OK` response is responded

✓ Data service providers 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

✓ Data service consumers MAY include a `Retry-After` header in the 503 response to indicate the expected unavailability of the service

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 protocol

✓ 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 communiceren in UTC-tijd

✓ Partijen MOETEN alle datums en tijdstippen vastgelegd in de generieke technische standaarden formatteren volgens het UNIX timestamp format

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

Grofmazig M2M Autorisatie Flow

- ✓ Datadienstgebruikers MOETEN een JWS maken volgens de [JWS specificaties](#)
- ✓ Datadienstaanbieders MOETEN de JWS valideren volgens de [JWS specificaties](#)

Informatiebeveiliging

- ✓ Partijen ZOULDEN een risicoanalyse uit MOETEN voeren
- ✓ Partijen ZOULDEN passende informatiebeveiligingsmaatregelen MOETEN nemen
- ✓ Partijen ZOULDEN 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 ZOULDEN 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 JWTs ondertekenen als een JSON Web Signature (JWS) zoals beschreven in [RFC 7515](#)
- ✓ Partijen MOETEN JWS formateren volgens JWS Compact Serialisation
- ✓ Partijen MOETEN het RS256 algoritme gebruiken bij het ondertekenen van een JWS
- ✓

Partijen MOETEN in JWS headers de parameters gebruiken zoals opgesteld in de onderstaande tabel. Partijen MOGEN andere parameters NIET gebruiken

✓ Partijen MOETEN een JWS payload "detached" maken van de handtekening, zoals beschreven in [RFC 7515 Appendix F](#)

✓ Partijen MOETEN JWS claims opstellen volgens het "JWT Bearer profile" als beschreven in [RFC 7523](#)

✓ Partijen MOETEN in JWS claims de parameters gebruiken zoals opgesteld in de onderstaande tabel

✓ Partijen ZOUDEN NIET andere JWS claims MOETEN definiëren en gebruiken, afhankelijk van het specifieke gebruik van de JWS

✓ Partijen MOETEN JWS claims binnen 30 seconden laten verlopen, aantoonbaar door de combinatie van `iat` en `exp` claims.

✓ Partijen MOETEN zowel `iat` als `exp` claims noteren in seconden en MOGEN `iat` en `exp` claims NIET noteren in milliseconden

✓ Partijen MOETEN een JWS maar één keer accepteren

✓ Partijen MOETEN een JWS 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 API requests

✓ Partijen MOETEN alle root certificaten voor QSEALS van CAs op de EU/EEA [List of Trusted Lists \(LOTL\)](#) en PKIO accepteren

Service Level Agreements

SLAs voor Deelnemers

✓ 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 ZOULDEN datadiensten binnen het beschikbaarheidsvenster minimaal 95% van de tijd beschikbaar MOETEN stellen aan datadienstgebruikers
- ✓ Datadienstaanbieders ZOULDEN op 95% van API verzoeken binnen 2 seconden MOETEN reageren binnen het beschikbaarheidsvenster
- ✓ Datadienstaanbieders ZOULDEN op 99% van API verzoeken binnen 5 seconden MOETEN reageren binnen het beschikbaarheidsvenster
- ✓ Datadienstaanbieders ZOULDEN ten minste 100 API verzoeken moeten kunnen verwerken binnen het beschikbaarheidsvenster
- ✓ Datadienstaanbieders MOETEN voor alle Prioriteit 1 en Prioriteit 2 incidenten een incident manager beschikbaar stellen
- ✓ Datadienstaanbieders ZOULDEN voor alle Prioriteit 1 en Prioriteit 2 incidenten een incident manager 24u per dag, 7 dagen per week beschikbaar MOETEN stellen
- ✓ Datadienstaanbieders MOETEN voor een Prioriteit 1 incident een update delen met de beheerorganisatie binnen 2 uur van elke belangrijke update en elke 4 uur
- ✓ Datadienstaanbieders MOETEN voor een Prioriteit 2 incident een update delen met de beheerorganisatie binnen 2 uur van elke belangrijke update aan het einde van elke werkdag
- ✓ Datadienstaanbieders MOETEN voor een Prioriteit 3 incident een volledige update delen met de beheerorganisatie aan het einde van elke werkdag
- ✓ Datadienstaanbieders ZOULDEN op een passende frequentie een back-up MOETEN maken van data belangrijk voor de datadienst
- ✓ Datadienstaanbieders ZOULDEN de back-ups MOETEN opslaan voor een passende periode
- ✓ Datadienstaanbieders ZOULDEN bereikbaar MOETEN zijn voor ondersteuning via e-mail
- ✓ Datadienstaanbieders ZOULDEN binnen een werkdag na ontvangst van een vraag, verzoek of klacht MOETEN aangeven dat hiervan kennis is genomen
- ✓ Datadienstaanbieders ZOULDEN binnen vijf werkdagen na ontvangst van een vraag, verzoek of klacht deze MOETEN beantwoorden of oplossen
- ✓ Datadienstaanbieders MOETEN aan alle releasebeheer eisen voldoen

Incidentenbeheer

- ✓ Partijen MOETEN incidenten direct na ontdekking melden bij de beheerorganisatie
- ✓ Datadienstaanbieders MOETEN de datum, tijd en ingeschatte incident classificatie, en impact op de datadienst melden bij de rapportage over een incident

✓ De beheerorganisatie MOET het incident beoordelen en legt het classificatie niveau vast

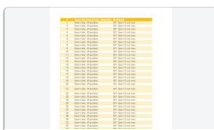
✓ Datadienstaanbieders MOETEN handelen volgens de SLAs bijhorende bij de vastgestelde classificatie van het incident

Marktvorzieningen

✓ Authenticatiediensten MOETEN voldoen aan alle eisen van een Identity Provider volgens [iSHARE](#)

✓ Autorisatieregisters MOETEN voldoen aan alle eisen van een Authorization Registry volgens [iSHARE](#)

Bijlage



230704A Overzi...n .xlsx
04 Jul 2023, 11:30 am

Begrippenlijst (Glossary)

Alle begrippen zijn in het Nederlands (links) en Engels (rechts) gedefinieerd, 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.

i 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](#).

i 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.

- Abonnement (Subscription)
- Access token
- Afsprakenstelsel (Trust framework)
- Afsprakenstelsel DSGO (DSGO trust framework)
- Application programming interface
- Authenticatie (Authentication)
- Authenticatiedienst (Authentication service)
- Autorisatie (Authorization)
- Autorisatiebeheer (Authorization management)
- Autorisatiebeleid (Authorization policy)
- Autorisatiebesluit (Authorization decision)
- Autorisatieregister (Authorization register)
- Beheerorganisatie DSGO (DSGO trust framework authority)
- Betrouwbaarheidsniveaus (Level of assurance)
- Data
- Datadienst (Data service)
- Datadienstaanbieder (Data service provider)
- Datadienstgebruiker (Data service consumer)
- Datadienst ontdekking (Data service discovery)
- Data delen (Data sharing)
- Deelnemer (Participant)
- Delegatie (Delegation)
- DSGO
- DSGO-programma (DSGO-programme)
- Ecosysteem (Ecosystem)
- EORI
- Event
- Federatief ecosysteem (Federated ecosystem)
- Human-to-machine
- Identificatie (Identification)
- Identificatiedienst (Identity Provider)
- Identifierend kenmerk (Identifier)

- Inlogmiddel (login)
- Interoperabiliteit (Interoperability)
- Marktvoorzieningen (Industry facilities)
- Notificatie (Notification)
- Machine-to-machine
- Rechthebbende (Entitled party)
- Resource
- Richtinggevende principes (Guiding principles)
- SLAs
- Stelselcatalogus (Trust framework catalog)
- Stelselvoorzieningen (Trust framework facilities)
- Voorzieningen (Facilities)

Abonnement (Subscription)

Een overeenkomst tussen een [datadienstaanbieder](#) en een [datadienstgebruiker](#) om [notificaties](#) te ontvangen over specifieke events gerelateerd aan een [datadienst](#).

An agreement between a [data service provider](#) and a [data service consumer](#) to receive [notifications](#) about specific events related to a [data service](#).

Bron (source): nvt (n/a)

Access token

Een 'string' met een specifiek toepassingsgebied, levensduur en andere toegangsvoorwaarde 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.

Bron (source): 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.

Trust frameworks are close collaborations of different parties from industry, government and science, which provide products or services, based on defined requirements.

Bron (source): Logius

Afsprakenstelsel DSGVO (DSGO trust framework)

Het [afsprakenstelsel DSGVO](#) is een set afspraken tussen [deelnemers](#) aan het DSGVO en is het fundament voor harmonisatie en vertrouwen om een [federatief ecosysteem](#) voor [data delen](#) te realiseren.

The DSGVO [trust framework](#) is a set of unified agreements between [participants](#) of the DSGVO and facilitates harmonisation and trust to realise a [federated ecosystem](#) for [data sharing](#).

Bron (source): nvt (n/a)

Application programming interface

Een application programming interface (API) is een gestructureerd en gedocumenteerd koppelvlak voor communicatie tussen applicaties.

Bron (Source): [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

Bron (source): [Data Sharing Coalition](#)

The process where the validity of a partij claiming an [identity](#) is verified.

Authenticatiedienst (Authentication service)

Een dienst voor het creëren, onderhouden, beheren en valideren van [identiteiten](#) ter behoeve van [authenticatie](#) voor partijen binnen het [afsprakenstelsel](#).

Bron (source): [Data Sharing Coalition](#)

A service for creating, maintaining, managing and validating [identities](#) for the purpose of [authentication](#) for parties within the [trust framework](#).

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.

Bron (source): [Data Sharing Coalition](#)

Having rights or permission and the process by which a party obtains rights or permission to perform a specific action.

Autorisatiebeheer (Authorization management)

De operationalisatie en de praktische implementatie van het [autorisatiebeleid](#).

Bron (source): nvt (n/a)

The operationalisation and practical implementation of the [authorisation policy](#)

Autorisatiebeleid (Authorization policy)

Per [datadienst](#) wordt autorisatiebeleid vastgelegd wat de logica en voorwaarde beschrijft waaraan moet worden voldaan om specifieke rechten te verkrijgen in de context van de dienst.

Bron (source): 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

The authorisation decision is the process whereby a [data service](#) request is validated against the requirements of the of the

autorisatiebeleid.

authorisation policy.

Bron (source): nvt (n/a)

Autorisatieregister (Authorization register)

De dienst waar de [autorisaties](#) en delegaties voor toegang tot een [datadienst](#) van [rechthebbende](#) is opgeslagen.

The service where [authorizations](#) and delegations for access to a [data service](#) of [entitled party](#) is stored.

Bron (source): iSHARE

Beheerorganisatie DSGO (DSGO trust framework authority)

De beheerorganisatie van het DSGO definieert en beheert het DSGO. Dit bevat het zorgen voor de doorontwikkeling van het [afsprakenstelsel](#), toezien op de naleving, toezien op de operatie van [voorzieningen](#) en beslechten van geschillen.

The DSGO trust framework authority defines and manages the DSGO. This includes ensuring the continued development of the [trust framework](#), monitoring compliance, overseeing the operation of [facilities](#), and resolving disputes.

Bron (source): Data Sharing Coalition

Betrouwbaarheidsniveaus (Level of assurance)

De mate waarin een geclaimde [identiteit](#) gegarandeerd kan worden.

The degree of confidence in the claimed [identity](#) of a person.

Bron (source): iSHARE

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.

Bron (source): Data Sharing Coalition

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](#).

Bron (source): Data Sharing Coalition

Datadienstaanbieder (Data service provider)

De partij die een [datadienst](#) aanbiedt aan de [datadienstgebruiker](#).

The party that offers a [data service](#) to the [data service consumer](#).

Bron (source): Data Sharing Coalition

Datadienstgebruiker (Data service consumer)

De partij die gebruik maakt van een door de [datadienstaanbieder](#) aangeboden [datadienst](#).

The party that makes use of a [data service](#) offered by the [data service provider](#).

Bron (source): [Data Sharing Coalition](#)

Datadienst ontdekking (Data service discovery)

Het mechanisme waarmee een [datadienstgebruiker](#) een [datadienst](#) en haar [datadienstaanbieder](#) kan vinden gebruikmakend van een [stelselcatalogus](#).

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 catalog](#).

Bron (source): [Data Sharing Coalition](#)

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](#).

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](#).

Bron (source): [Data Sharing Coalition](#)

Deelnemer (Participant)

Deelnemers (aan het [afsprakenstelsel](#)) zijn partijen die zich hebben aangesloten bij het [afsprakenstelsel](#) en zich houden aan de gemaakte [afspraken](#).

([Trust framework](#)) participants are parties which have joined the [trust framework](#) and adhere to its [agreements](#)

Bron (source): [Data Sharing Coalition](#)

Delegatie (Delegation)

Het overdragen van een [bevoegdheid](#) aan een ander dat de [bevoegdheid](#) gaat uitoefenen.

Transferring a [power](#) to another person who will exercise the [power](#).

Bron (source): nvt (n/a)

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](#).

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](#).

Bron (source): nvt (n/a)

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.

Bron (source): 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.

a distributed, adaptive, open system with properties of self-organisation, scalability and sustainability.

Bron (source): nvt (n/a)

EORI

Een Europees identificatienummer dat binnen de EU wordt gebruikt om partijen op uniforme wijze te [identificeren](#).

An European identification number that is used to [identify](#) parties in a uniform manner with the EU.

Bron (source): [Belastingdienst](#)

Event

Een gedefinieerde specifieke gebeurtenis in de bronsystemen van een [datadienstaanbieder](#). Bijvoorbeeld het wijzigen van de brondata.

A defined specific occurrence in the source systems of a [data service provider](#). For example, the modification of the data.

Bron (source): nvt (n/a)

Federatief ecosysteem (Federated ecosystem)

Een [ecosysteem](#) waar partijen in verschillende rollen samenwerken en op elkaar vertrouwen terwijl ze hun eigen zelfstandigheid houden.

An [ecosystem](#) where parties in various roles cooperate and trust each other while maintaining their own independence.

Bron (source): nvt (n/a)

Human-to-machine

Een human-to-machine interactie is een interactie waarbij een persoon met een machine communiceert middels een user-interface.

A human-to-machine interaction is one in which a person communicates with a machine through a user-interface.

Bron (source): nvt (n/a)

Identificatie (Identification)

het proces waarbij een identiteit wordt aangeduid aan of wordt geclaimd door een partij die een rol vervuld in het [afsprakenstelsel](#).

The process by which an identity is designated to or is claimed by a party fulfilling a role within the [trust framework](#).

Bron (source): [iSHARE](#)

Identificatiedienst (Identity Provider)

Zie [Authenticatiedienst](#)

see [Authentication service](#)

Bron (source): [iSHARE](#)

Identificerend kenmerk (Identifier)

Een uitdrukking van een identiteit.

An expression of an identity.

Bron (source): nvt (n/a)

Inlogmiddel (login)

Nader nog uit te werken

To be determined

Bron (source): nvt (n/a)

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.

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.

Bron (source): [New European Interoperability Framework](#)

Marktvoorzieningen (Industry facilities)

[Voorzieningen](#) die geleverd worden door marktpartijen in de gebouwde omgeving

[Facilities](#) which are provided by the industry parties in the built environment

Bron (source): nvt (n/a)

Notificatie (Notification)

Een melding van een event van de [datadienstaanbieder](#), ontvangen door de [datadienstgebruiker](#) onder de voorwaarde van een [abonnement](#).

A notification of an event from the [data service provider](#), received by the [data service consumer](#) under the condition of a [subscription](#).

Bron (source): nvt (n/a)

Machine-to-machine

Een machine-to-machine interactie is een interactie tussen twee machines zonder tussenkomst van een persoon.

A machine-to-machine interaction is an interaction between two machines without the intervention of a person.

Bron (source): nvt (n/a)

Rechthebbende (Entitled party)

De entiteit die rechten heeft om te bepalen wat er met [data](#) gebeurt. Het is taak van de [datadienstaanbieder](#) om te weten wie rechthebbend is/zijn.

The entity that has rights to determine what happens to [data](#). It is task of the [data service provider](#) to know which entity/entities is/are entitled.

Bron (source): [Data Sharing Coalition](#)

Resource

Een resource is een object met een type, bijbehorende [data](#), relaties met andere resources en een aantal operaties om deze te bewerken.

A resource is an object with a type, associated [data](#), relationships to other resources and operations to manipulate it.

Bron (source): [Geonovum Nederlandse API Strategie](#)

Richtinggevende principes (Guiding principles)

Principes die richting geven aan besluiten over afspraken gedurende het vaststellen en onderhouden van het [afsprakenstelsel](#).

Principles that give direction in the decision-making process of establishing and maintaining the [trust framework](#).

Bron (source): [Data Sharing Coalition](#)

SLAs

Servicelevel-overeenkomsten (of dienstenniveau-overeenkomsten) zijn afspraken over de kwaliteit, beschikbaarheid en verantwoordelijkheden van [datadiensten](#).

Service Level Agreements are agreements on the quality, availability and responsibilities of [data services](#).

Bron (source): nvt (n/a)

Stelselcatalogus (Trust framework catalog)

Catalogus die alle nodige informatie bevat om [datadiensten](#), [deelnemers](#), en [voorzieningen](#) te vinden, begrijpen en gebruiken.

Catalog that contains all necessary information to find, understand, and make use of [data services](#), [participants](#), and [facilities](#).

Bron (source): nvt (n/a)

Stelselvoorzieningen (Trust framework facilities)

Voorzieningen die geleverd worden door de beheerorganisatie van het DSGO.

Facilities which are provided by the DSGO trust framework authority.

Bron (source): nvt (n/a)

Voorzieningen (Facilities)

Componenten die ondersteunende functionaliteiten bieden die nodig zijn voor het functioneren van het DSGO. Zoals bijvoorbeeld een autorisatieregister, authenticatiedienst en de stelselcatalogus.

Components that provide supporting functionalities necessary for the operation of the DSGO. For example, an [authorization register](#), [authentication service](#) and the [scheme catalog](#).

Bron (source): nvt (n/a)

FAQ

Deze sectie bevat een overzicht van enkele veel gestelde vragen met antwoorden:

▼ Wat is een afsprakenstelsel?

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.

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.

Voor meer informatie zie deze pagina's

[Doel van het Digitaal Stelsel Gebouwde Omgeving](#)

[Kern van het Afsprakenstelsel](#)

[Het BLOFT-raamwerk](#)

▼ Wat is de rol van richtinggevende principes in het DSGO?

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**.

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.

Voor meer informatie zie deze pagina:

[Richtinggevende Principes](#)

▼ Zal het toekomstige DSGO interoperabel zijn met andere initiatieven?

Het **DSGO-programma** houdt (**datadeel**) ontwikkelingen buiten de gebouwde omgeving in de gaten. De **richtinggevende principes** borgen dat het **DSGO** streeft om **interoperabel** te zijn. Echter, het **DSGO** is niet verantwoordelijk voor afhankelijkheden met andere sectoren. Wanneer dit relevant is voor een specifieke use case zal dit worden meegenomen in mogelijk specifieke afspraken.

Voor meer informatie zie deze pagina's:

[Richtinggevende Principes](#)

[Aanpak ontwikkeling afsprakenstelsel DSGO](#)

▼ Hoe wordt het afsprakenstelsel DSGO verder ontwikkeld?

Aankomende periode gaat het **DSGO-programma** samen met partijen uit de gebouwde omgeving generieke onderwerpen ontwikkelen in werkgroepen. Parallel zal aan de hand van concrete use cases specifieke afspraken worden ontwikkeld.

Voor meer informatie zie deze pagina's:

[Aanpak ontwikkeling afsprakenstelsel DSGO](#)

[Specifieke Functionaliteiten](#)

▼ Hoe wordt het DSGO beheerd?

Tijdens de looptijd van het **DSGO-programma** wordt het afsprakenstelsel beheerd door het **DSGO** projectteam Afsprakenstelsel. In een apart project binnen het **DSGO-programma**, wordt de governance en processen van de toekomstige **beheerorganisatie** uitgewerkt.

Voor meer informatie zie deze pagina:

[Beheer](#)

▼ Waarom is er op dit moment weinig focus op specifieke afspraken?

Specifieke afspraken in het [afsprakenstelsel](#) zullen aan de hand van use cases worden ontwikkeld. Sinds het begin van [DSGO-programma](#) is het programma in gesprek met partijen uit de gebouwde omgeving om tot use cases te komen om aan de hand daarvan specifieke afspraken uit te werken. Deze zijn afgelopen maanden naar een punt gebracht waarop ze binnenkort kunnen leiden tot specifieke afspraken, indien dit nodig is voor de use case. Om voortgang te maken, zijn tot die tijd de eerste generieke afspraken opgesteld.

Voor meer informatie zie deze pagina's:

[Aanpak ontwikkeling afsprakenstelsel DSGO](#)

[Specifieke Functionaliteiten](#)

▼ 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](#). Het is de verantwoordelijkheid van een datadienstaanbieder om een datadienst te definiëren en implementeren binnen de kaders van het afsprakenstelsel.

Voor meer informatie zie de pagina's

[Wat is een datadienst?](#)

[Rollenmodel](#)

▼ Hoe verhoudt semantiek zich tot het afsprakenstelsel DSGO?

Wanneer data [wordt gedeeld](#) is een gedeeld begrip van de semantiek van de gedeelde data essentieel. Op dit moment bevat het [afsprakenstelsel DSGO](#) geen semantische afspraken. 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. Daarom kunnen generieke afspraken niet over de semantische inhoud van [datadiensten](#) gaan.

In use cases, kan er een behoefte ontstaan voor afspraken rondom semantiek. In dat geval zou het kunnen dat dit als specifieke afspraak in het afsprakenstelsel wordt opgenomen indien nodig. Dat betekent niet dat voor elke use case afspraken over een volledig semantisch model wordt vast gelegd, maar het is een mogelijkheid.

Voor meer informatie zie deze pagina's

[Scope van het Digitaal Stelsel Gebouwde Omgeving](#)

[Aanpak ontwikkeling 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 zal dit [publiekelijk](#) worden gecommuniceerd.

▼ 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 [autorisatiebeleid](#), [autorisatiebeheer](#), en [autorisatiebesluit](#). Voor elke [datadienst](#) moet een autorisatiebesluit worden genomen. Om dit te doen moet de [datadienstaanbieder](#)

informatie van het datadienstverzoek toetsen tegen het autorisatiebeleid. Informatie die hiervoor nodig kan zijn, zijn is geregistreerde delegaties. [Delegatie](#) is het overdragen van een bevoegdheid aan een ander die de bevoegdheid gaat uitoefenen.

Voor meer informatie zie deze pagina's

[Autorisatiebeleid](#)

[Autorisatiebeheer](#)

[Autorisatiebeheer](#)

▼ 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

[Autorisatiebeheer](#)

▼ 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

[Autorisatiebeheer](#)

▼ Wat houdt een abonnement op een datadienst in?

Het [DSGO](#) legt met afspraken een fundament waarop partijen [datadiensten](#) kunnen definiëren om data te delen of te bewerken. Het [DSGO](#) definieert een [abonnement](#) als een standaard datadienst. Een abonnement is een overeenkomst tussen een [datadienstaanbieder](#) en datadienstgebruiker om [notificaties](#) te ontvangen over specifieke events gerelateerd aan een datadienst. Datadienstaanbieders zijn niet verplicht een abonnement te implementeren.

Voor meer informatie zie de pagina

[Abonnement op een Datadienst](#)

▼ 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 data te delen. De komende maanden wordt het [DSGO](#) doorontwikkeld naar een meer volwassen stelsel. 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 afsprakenstelsel DSGO](#)

▼ Hoe ziet het contract wat de deelnemers tekenen eruit?

Dat hangt uiteindelijk van de [deelnemers](#) zelf af, maar het contract zal waarschijnlijk vooral verwijzen naar het [afsprakenstelsel](#) en zelf weinig nieuwe bepalingen bevatten. Het zal dan een deelnameovereenkomst zijn waarin de partij die van het afsprakenstelsel gebruik wil maken zich vrijwillig en eenzijdig jegens de [DSGO-beheerorganisatie](#) bindt aan de in het afsprakenstelsel opgestelde rechten en plichten. Het contract is vervolgens alleen van toepassing wanneer de partij uitdrukkelijk aangeeft data te delen op de door [DSGO](#) voorgeschreven manier. Er zit geen minimale gebruiks- of afnameverplichting of exclusiviteitsclausule in. Het contract is slechts

bedoeld om te waarborgen dat alle aangesloten partijen op dezelfde voorgeschreven manier handelen wanneer “onder de vlag van DSGVO” data gedeeld wordt.

Bijlage

