Programma
Aan de slag met de
Omgevingswet

Deelprogramma
Digitaal Stelsel Omgevingswet

Globale Architectuur Schets
Knooppunt Gegevensuitwisseling

Versie 2.0 Definitief 9 januari 2020

Colofon

Titel	:	Globale Architectuur Schets Knooppunt Gegevensuitwisseling
Versie	:	2.0 Definitief
Datum	:	9 januari 2020
Opdrachtgever	:	Programma Implementatie Omgevingswet
Opdrachtnemer	:	Deelprogramma DSO
Auteurs	:	Bas Crompvoets *Domeinarchitect PDSO* Jan Jaap Zoutendijk *Projectarchitect*
Contactpersoon	:	Kadaster Tactisch Beheer Organisatie TBO-DSO-LV@kadaster.nl
Gebaseerd op	:	Visie 1.0 Programma van eisen 2.4 Doelarchitectuur 3.11 Globaal Content Raamwerk 1.1 Overall GAS 2.0

Versiehistorie

Versie	Status	Datum	Auteur(s)	Toelichting
1.6	Concept	24-01-2018	F. Terpstra	Actualisering op Doelarchitectuur 2.0 en OGAS1.5
1.9	Concept	04-11-2019	B. Crompvoets, J.J. Zoutendijk	Actualisering op het nieuwe GAS template tbv overdracht TBO.
1.92	Concept	22-11-2019	B. Crompvoets, J.J. Zoutendijk	Versie opgeleverd ter review.
1.93	Concept	26-11-2019	B. Crompvoets, J.J. Zoutendijk	Tussenversie: reviewcommentaar Provincies, Gemeenten en Waterschappen verwerkt
2.0	Definitief	09-01-2020	B. Crompvoets, J.J. Zoutendijk	Oplevering Major Release

Goedkeuring

Functie	Naam	Versie	Datum	Handtekening
Stelselarchitect namens het Opdrachtgevend Beraad	René Kint	2.0		
Programmadirecteur Implementatie Omgevingswet namens de Programmaraad	Bert Uffen	2.0		
Lead architect programma	Anton van Weel	2.0		

Distributie

Functie/Orgaan	Versie	Opmerkingen
Programmaraad Implementatie Omgevingswet	2.0	
Stelsel Architectuur Board (SAB)	2.0	
Stelsel Architectuur Team (SAT)	2.0	
Programma/Project Architectuur Team (PAT)	2.0	
Productowners/Productarchitecten	2.0	
Strategische Ontwikkelpartners (senior supplier)	2.0	

Review

Naam	Versies
SAT	1.92
Productarchitect	1.90, 1.92

Inhoudsopgave

1 Inleiding

Dit document bevat de *Globale Architectuur Schets* (GAS) voor het componentcluster Knooppunt Gegevensuitwisseling.

De primaire verantwoordelijkheid die aan het componentcluster Knooppunt Gegevensuitwisseling is toegekend bestaat uit drie delen:

- *"Overheden sluiten aan via een centraal aansluitpunt wat de complexiteit vermindert"*
- *"Centrale functionaliteiten om gegevens te ontvangen en verstrekken in en buiten het DSO."*
- *"Belangrijk is dat het digitaal stelsel niet één groot ICT-systeem is, maar een samenhangend stelsel van digitale voorzieningen."*

Tot slot wordt invulling gegeven aan de "Robuust" eis uit de doelarchitectuur. Die wordt gesteld aan het onderdeel "Gegevens ontsluiten" waar het knooppunt onder valt

De functionaliteit van het Knooppunt is intern gericht, dat wil zeggen: het ontsluit alleen de services van het stelsel. De aanbieders binnen het stelsel bepalen hoe de functionaliteit wordt geleverd. Afnemers van services van het stelsel hebben via het Knooppunt één generiek toegangspunt tot het stelsel. Zij kunnen de configuratie van de Knooppunt functionaliteiten maar zeer beperkt beïnvloeden.

"Overheden sluiten aan via een centraal aansluitpunt wat de complexiteit vermindert"
*Deze doelstelling w*ordt gerealiseerd doordat Het Knooppunt alle services van alle onderdelen van het stelsel Omgevingswet op een eenduidige manier ontsluit. Via het Knooppunt acteert dit stelsel als één geheel. Alle services zijn op één plek te vinden en af te nemen. Een afnemer hoeft slechts te verbinden met één Knooppunt en niet met vele aanbieders. Omgekeerd hoeft een aanbieder ook slechts te verbinden met één Knooppunt en niet met vele afnemers.

"Centrale functionaliteiten om gegevens te ontvangen en verstrekken in en buiten het DSO."
Uit de eerste doelstelling volgt de volgende doelstelling: Deze centraal gepositioneerde functionaliteit moet geen knelpunt zijn en dus efficiënt verlopen. Het centraal ontsluiten van services via het Knooppunt verloopt efficiënt doordat zowel afnemers als aanbieders via een zelfbedieningsfunctionaliteit services via het Knooppunt kunnen afnemen of aanbieden. Het technisch aansluiten doen afnemers en aanbieders dus zelf. Het beheer van de tot stand gebrachte verbindingen in het stelsel wordt daarnaast centraal ondersteund vanuit de beheerorganisatie van het Knooppunt.

"Belangrijk is dat het digitaal stelsel niet één groot ICT-systeem is, maar een samenhangend stelsel van digitale voorzieningen."
Een hoge mate van zelfbediening kan alleen worden bereikt als hiermee rekening gehouden wordt. Het knooppunt is hierbij afhankelijk van het bestaan van een proces dat toetst op de samenhang en kwaliteit. Als dit proces er is kan het Knooppunt deze

ondersteunen door alleen services tot het knooppunt toe te laten die getoetst zijn op samenhang en kwaliteit.

Nadat aanbieder en afnemer via zelfbediening met elkaar verbonden zijn, begint het daadwerkelijke afnemen. Het Knooppunt geeft hierbij invulling aan de **"robuust"** doelstelling. Het hoeft in de loop der tijd niet of nauwelijks aangepast te worden. De dynamiek in het stelsel zit in de gebruikerstoepassingen, in het gegevens inwinnen en in het gegevens verstrekken. Het Knooppunt zorgt voor het ontkoppelpunt voor de logistiek van berichten (envelop) en in sommige gevallen[1] ook voor de inhoud van berichten. Hierdoor kunnen de gebruikerstoepassingen en toepassingen voor het inwinnen en verstrekken van gegevens onafhankelijk van elkaar worden aangepast. Daarnaast biedt het Knooppunt eenduidige wijze van beveiliging en routering, rapportages over gebruik en ondersteuning bij het leveren van informatie voor verantwoording over het berichtenverkeer die kan worden gebruikt in de processen van bezwaar en beroep.

Soorten services
Het stelsel onderscheidt vier soorten services. Onderstaande tabel biedt een overzicht hiervan op basis van de onderscheidende kenmerken in gebruik.

Type services	Registreren voor afname service	Toetsen toegang	Beveiliging
Open service anoniem	Nee	N.v.t.	Anoniem beveiligd (met API-key)
Open service met service garanties	Ja	Automatisch indien aangemeld bij stelsel	Beveiligd met laag niveau authenticatie middel
Service met toegangsbeperking	Ja	Automatisch indien aangemeld bij stelsel met juiste rol	Beveiligd met midden niveau authenticatie middel
Service met doelbinding	Ja	Handmatig proces met aanbieder	Beveiligd met hoog niveau authenticatie middel

Ten eerste kent het Knooppunt de mogelijkheid open services anoniem en zonder service garanties aan te bieden. Anonieme open services bevatten alleen open data en worden laagdrempelig aangeboden (API-key). In hun SLA wordt de beschikbaarheid aangeduid met termen als best effort en fair use.
Overige services kennen een servicegarantie en vereisen registratie voor afname. Services met servicegaranties kennen geen anoniem gebruik, bij gebruik is authenticatie vereist.

Daarnaast zijn er services die niet voor alle gebruikers in het stelsel toegankelijk zijn. Het gaat hierbij om services die alleen toegankelijk zijn voor een bepaalde rol binnen het stelsel, bijvoorbeeld bevoegd gezag of applicatie functies. Afhankelijk van de aard van de informatie die deze service levert, gaat het dan om een service met toegangsbeperking of een service met doelbinding.

[1] Het knooppunt bevat geen businesslogica, de mogelijkheden voor vertalen van berichtinhoud is daarmee beperkt. Vertalingen worden alleen ontwikkeld op verzoek van componenten binnen het DSO.

1.1 *Doel en resultaat*

Het doel van een GAS is het beschrijven van de globale architectuur en de keuzen die daarin voor het component Knooppunt Gegevensuitwisseling gemaakt zijn.
De GAS bevat de hoofdkeuzen voor de te ontwikkelen oplossing. Daarnaast zorgt de GAS dat de oplossing aansluit op architectuur van de interbestuurlijke partners (Rijk, provincies, gemeenten en waterschappen). Dit geheel zorgt ervoor dat de veranderopgave in samenhang met andere veranderingen wordt gerealiseerd en past binnen de gewenste toekomst vaste informatievoorziening van het Digitaal Stelsel Omgevingswet (DSO).

Een GAS stelt de opdrachtgever in staat gedurende het opstellen ervan besluiten te nemen over onderkende architectuurkeuzen. De PSA (Project Start Architectuur) werkt de GAS uit voor de hele breedte van de oplossing. De PSA is gehouden aan de oplossingsrichting en de kaders beschreven in deze GAS en kan hiervan niet afwijken zonder akkoord van de Stelsel Architectuur Board (SAB) van het DSO.

De Overall GAS (OGAS) is de overkoepelende kapstok met algemene kaders en richtlijnen voor het stelsel waar elke GAS aan moet voldoen om een digitaal stelsel te realiseren dat werkt en op een eenduidige en samenhangende manier is opgezet.

1.2 *Samenhang andere documenten*

De laatste versie van het document 'DSO – Architectuur – Governance' licht toe hoe de GAS samenhangt met bovenliggende kaders en andere architectuurdocumenten.

1.3 *Leeswijzer*

In hoofdstuk 2 t/m 6 worden respectievelijk de lagen Grondslagen, Organisatie, Informatie, Applicatie en Netwerk beschreven.

In hoofdstuk 7 worden de Beheeraspecten beschreven.

In hoofdstuk 8 worden de aanvullingen/uitzonderingen op de beveiliging en privacy (benoemd in de OGAS) beschreven die van toepassing zijn voor deze GAS.

In hoofdstuk 9 worden de aanvullingen/uitzonderingen op de transitie (benoemd in de OGAS) beschreven die van toepassing zijn voor deze GAS.

Bijlage A betreft de lijst met bronnen die voor het opstellen van deze GAS gebruikt zijn.

2 Grondslagen

In dit hoofdstuk wordt ingegaan op de kaders die van toepassing zijn op de positie en rol van Knooppunt Gegevensuitwisseling, waarbinnen de dienstverlening plaatsvindt. Het is een beschrijving in brede zin, dat wil zeggen de wat en hiermee onafhankelijk van de te kiezen oplossing. De algemeen geldende grondslagen staan beschreven in het OGAS. In dit hoofdstuk wordt ingegaan op aanvullingen en afwijkingen van deze algemene grondslagen.

2.1 *Grondslagen*

In deze paragraaf worden de aanvullingen/uitzonderingen op de algemene grondslagen (benoemd in de OGAS) beschreven die van toepassing zijn voor deze GAS.

In principe zijn er geen specifieke grondslagen voor het Knooppunt. De meeste kadering is overheidsbeleid zoals standaardisatie, hergebruik eOverheidscomponenten en baseline informatiebeveiliging overheid (BIO).

Wettelijke kaders die wèl van toepassing zijn omvatten:

- Archiefwet
  Gezien de taak van gegevensuitwisseling ontstaat er logistieke informatie die (mogelijk) gearchiveerd dient te worden.
- Algemene Verordening Gegevensbescherming (AVG).
- eIDAS
  Europese verordening voor Trust services.

2.2 *Principes*

In deze paragraaf worden de aanvullingen/uitzonderingen op principes (benoemd in de OGAS) beschreven die van toepassing zijn voor deze GAS.

DSO01	
Statement	De Klant staat centraal
Eisen	Zelfbediening wordt gebruikt om zowel beheerders als gebruikers te faciliteren.

DSO02	
Statement	Het stelsel functioneert als 1 geheel voor zowel personen als systemen.
Eisen	- Alle stelsel services worden via het Knooppunt ontsloten. Er komt bestuurlijke, functionele en technische afstemming tussen het DSO Knooppunt en aangesloten sectorale knooppunten om te zorgen dat de knooppunten voor de

	gebruiker als één geheel functioneren. Het Knooppunt geeft invulling aan dit centrale aanspreekpunt

DSO04	
Statement	Oplossingen zijn eenvoudig, generiek en kosten effectief.
Eisen	Business logica wordt nooit in het Knooppunt opgelost, maar in de achterliggende services van stelselvoorzieningen. Als dit business functionaliteit betreft die door meerdere stelselvoorzieningen wordt gebruikt, dan wordt door de governance van het DSO een keuze gemaakt welke stelselvoorziening de functionaliteit oplost en de andere maken via het Knooppunt gebruik van de services die deze stelselvoorziening levert.

DSO05	
Statement	Alles is een service
Eisen	- Het Knooppunt is de hoofdingang voor gebruikers van stelsel services. - Open datasets zijn in hun geheel als download beschikbaar bij de bron als ook via data.overheid.nl. - Het is toegestaan open services via het Knooppunt aan derden aan te bieden. - Open services bevatten alleen open data - Open services zijn laagdrempelig en zijn met slechts registratie door middel van een API-key te bevragen. - Afnemers en aanbieders regelen de migratie tussen versies zelf via zelfbediening op het Knooppunt

DSO06	
Statement	Het stelsel is open, transparant en innoverend.
Eisen	Alle stelsel services worden via het Knooppunt ontsloten. De services die intern binnen het stelsel worden gebruikt worden ook via het Open Stelsel aan de buitenwereld aangeboden zodat de markt zelf waarde toevoegende toepassingen kan maken.

DSO07	
Statement	Hergebruik voor koop voor maak
Eisen	Er wordt gebruik gemaakt voor de realisatie van zoveel mogelijk standaard cloud componenten (WSO2).

DSO08	
Statement	Continuïteit wordt geborgd
Eisen	Bestaande standaarden voor het volgen van berichten in de keten worden gevolgd waaronder StUF-ZKN. Daar waar binnen de bestaande standaard geen afspraken zijn moeten die gemaakt worden voor het gebruik van die standaard binnen het DSO.

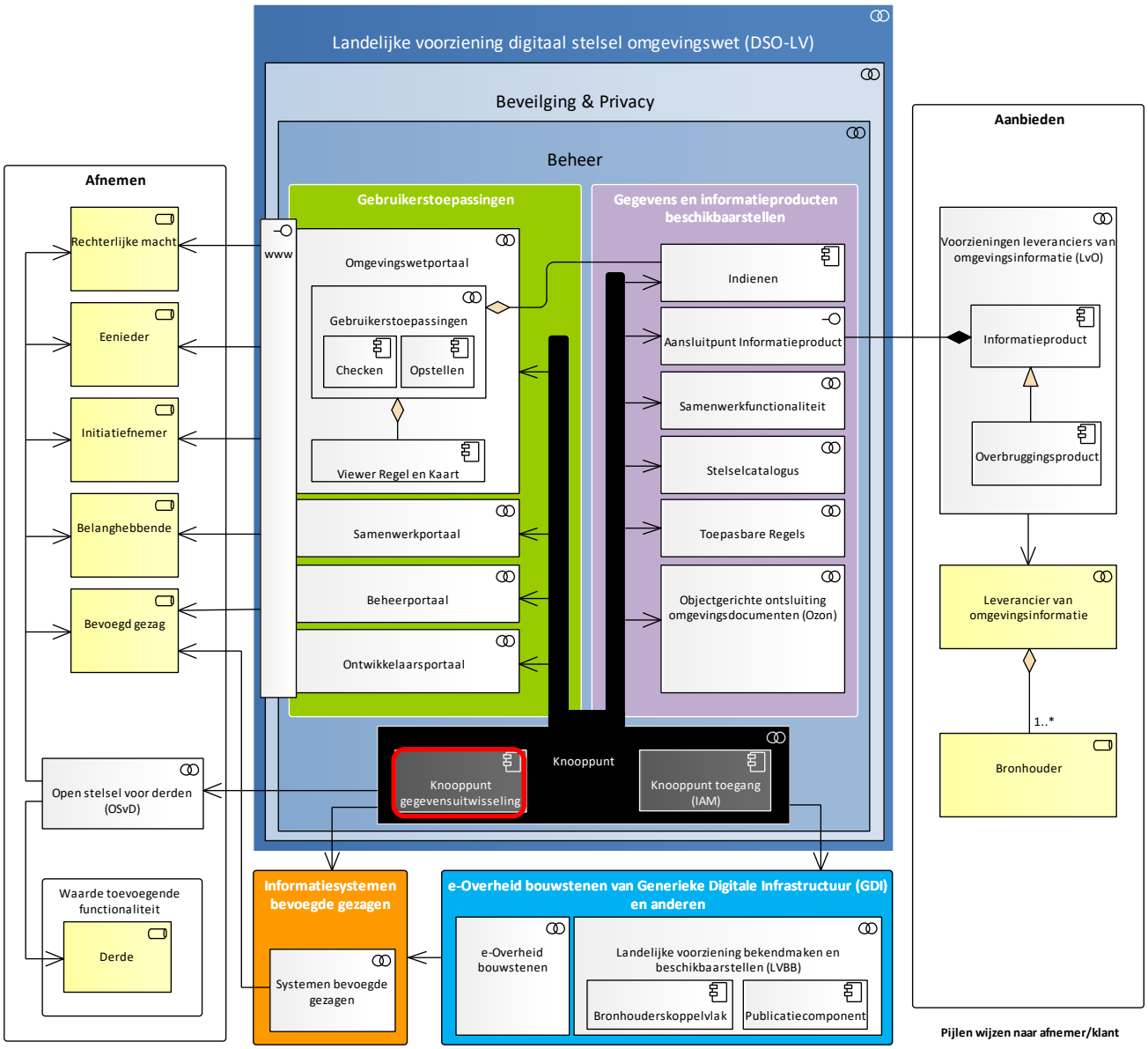
DSO09	
Statement	Passende beveiliging voor reële risico's.
Eisen	Het Knooppunt geeft waar nodig identiteitsinformatie van de afnemer door aan de service aanbieder zodat acties op het juiste niveau herleidbaar zijn. Het Knooppunt ondersteunt Digikoppeling. In aanvulling op berichtarchivering en auditing wordt tekenen van berichten toegepast daar waar de zwaarste eisen aan onweerlegbaarheid worden gesteld.

DSO10	
Statement	Beheerfunctionaliteit is primaire functionaliteit
Eisen	- Het Knooppunt verzamelt statistieken over het gebruik van stelsel services, kan aantonen of servicelevels worden gehaald en rapporteert hierover. - Alle stelsel services zijn op het Knooppunt bekend. - Servicelevels zijn binnen het DSO opgesteld en bestuurlijk bekrachtigd. - Er zijn kwaliteitseisen waarin services moeten voldoen voordat ze in productie mogen. Deze kwaliteitseisen worden binnen het DSO getoetst.

3 Organisatie

In dit hoofdstuk wordt de Organisatielaag beschreven van Knooppunt Gegevensuitwisseling, deze is bepalend voor de te kiezen oplossingen. Dit hoofdstuk positioneert de GAS Knooppunt Gegevensuitwisseling in het stelsel, waarin de ketens uit de OGAS als basis zijn gebruikt. In onderstaande figuur is met de rode omlijning weergegeven welke capabilities in deze keten worden ondersteund.

De GAS kan als volgt worden gepositioneerd waarbij onderstaand diagram tot uiting brengt dat Knooppunt Gegevensuitwisseling ondersteunend is aan de andere DSO-LV componenten:



Figuur 1 Overall architectuur DSO-LV

Vrijwel alle services binnen het stelsel lopen via het Knooppunt. Alle organisatie(onderdelen) die iets met services doen en de applicaties en services die zij beheren[2], hebben met het Knooppunt te maken. Deze organisaties worden geraakt in hun ontwikkelproces, tijdens gebruik en bij wijzigingen.

De verschillende rollen en organisaties die binnen deze context vallen worden in de tabellen hieronder toegelicht.

Rollen

#	Rol	Toelichting
1	Aanbieder	Aanbieders ontwikkelen services en stellen die beschikbaar voor gebruik in het stelsel.
2	Afnemer	Afnemers (binnen en buiten het stelsel) ontwikkelen applicaties die services uit het stelsel afnemen.
3	Bevoegd gezag	Bevoegd gezagen sluiten via het Knooppunt aan op het stelsel
4	Derden	Derden zijn afnemers van het stelsel die via een app of applicatie ontwikkeld buiten het DSO koppelen met het DSO. Dit wordt nader uitgewerkt in het project Open stelsel voor derden (PR10). Een applicatie van een derde kan acteren namens een burger, bedrijf of overheid in de rol van initiatiefnemer, belanghebbende of bevoegd gezag.
5	Stelselbeheerder	De Stelselbeheerder zorgt voor sturing in het stelsel. Ze bewaakt de goede werking van het stelsel. Hiervoor wordt informatie over de werking van het stelsel verzamelt. In overleg met verschillende stakeholders worden maatregelen genomen voor verbetering van de werking van het stelsel.
6	Opdrachtgever	De opdrachtgever kan via servicemanagement sturen op operationeel en tactisch beheer van het Knooppunt.

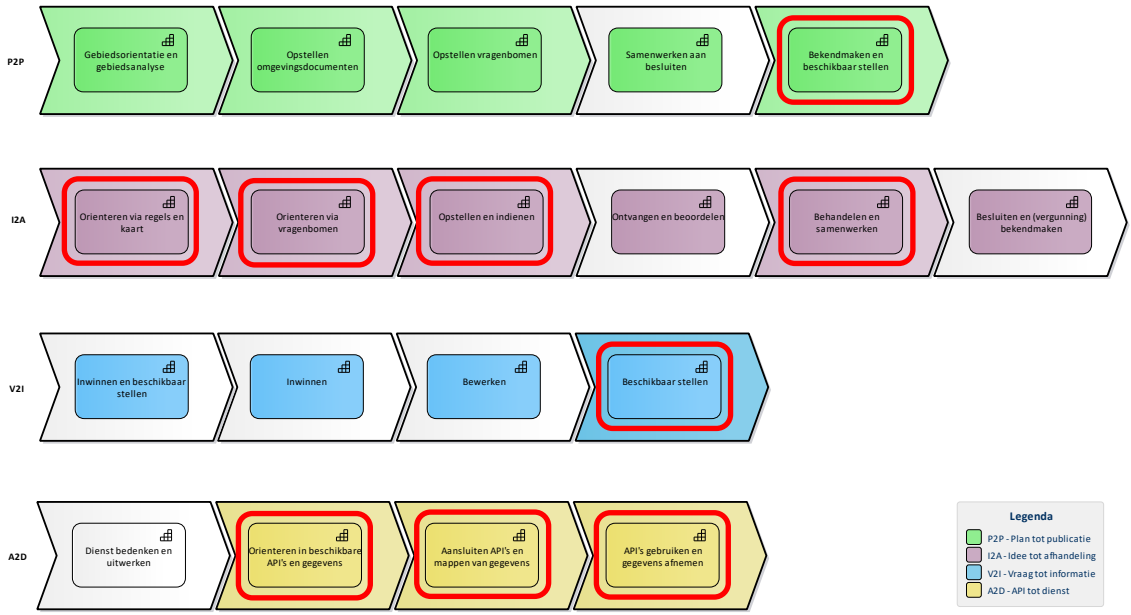
Organisaties

#	Organisatie	Toelichting
1	Strategische (en tactische/operationele) ontwikkel- en beheerpartners	Ontwikkelen stelselonderdelen die services realiseren die via het Knooppunt worden aangeboden. Heeft voor het Knooppunt primair de rol van aanbieder.
3	Serviceorganisatie	De serviceorganisatie is het centrale aanspreekpunt van het stelsel. De serviceorganisatie moet samenwerken met de beheerorganisatie van het Knooppunt voor het ondersteunen van gebruik en de verbetering en doorontwikkeling van het Knooppunt. Voor het Knooppunt vervult deze de rol van Stelselbeheerder. Daarnaast maakt de serviceorganisatie o.a. gebruik van het Knooppunt voor het rapporteren over het gebruik van het stelsel.
4	Interbestuurlijke partners	De interbestuurlijke partners (Rijk, provincies, gemeenten en waterschappen). Zijn opdrachtgever voor het stelsel en dus ook voor het Knooppunt.

[2] Er is een strategisch issue gedefinieerd over de manier waarop koepels aansluiten op het Knooppunt. Dit kan via eigen sectorale knooppunten of rechtstreeks. De uitkomst hiervan heeft geen invloed op de functionaliteit in dit document beschreven.

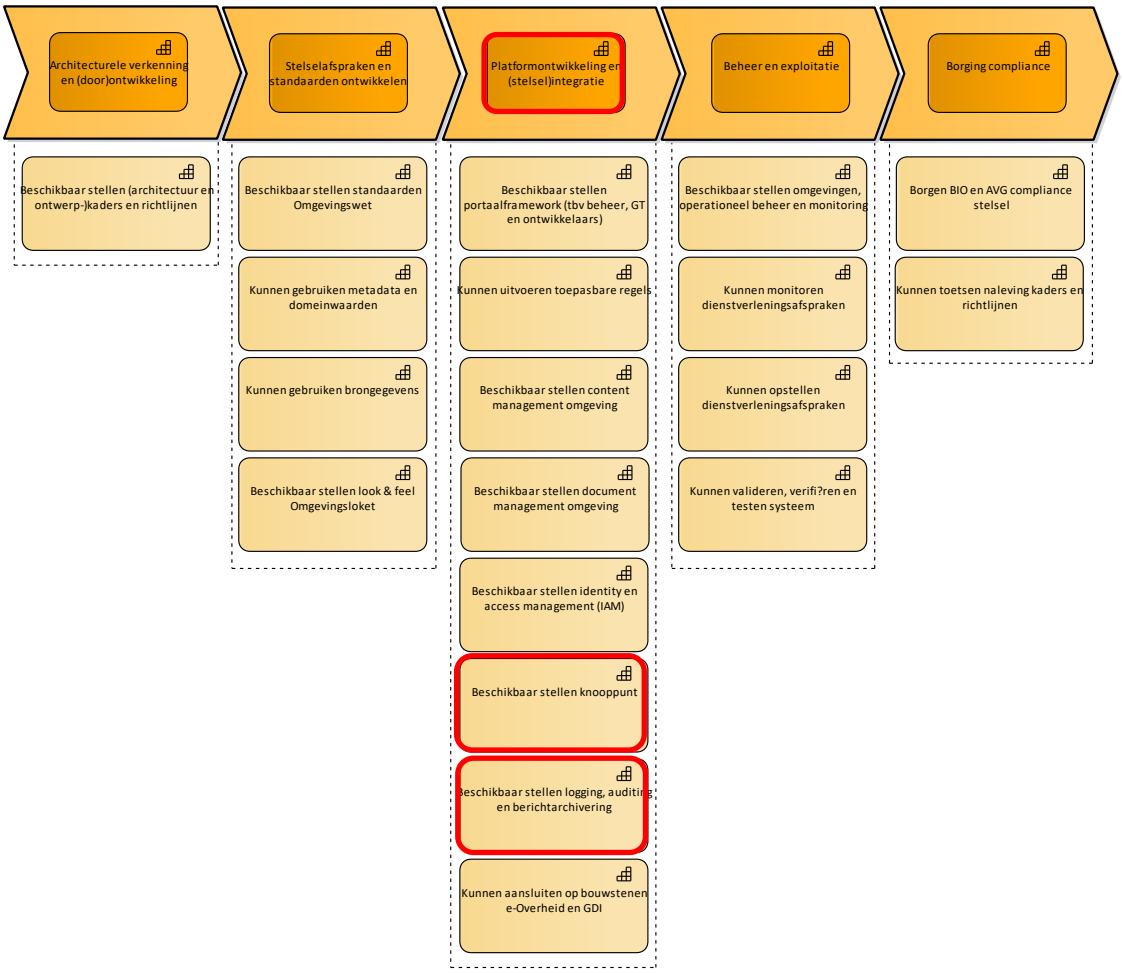
3.1 *Overzicht capabilities*

In deze paragraaf wordt de positionering en de context van Knooppunt Gegevensuitwisseling t.o.v. van het gehele stelsel weergegeven. Het stelsel wordt hier beschouwd vanuit de relevante waardeketens en de bijbehorende specifieke capabilities. De rode omkadering geeft aan welke capabilities ondersteund worden.



Figuur 2 Capabilities

Zoals uit bovenstaande ook al duidelijk wordt is het knooppunt echter primair een enabling capability.



Figuur 3 Enabling capabilities

Deze enkelvoudige presentatie doet echter geen recht aan de brede set van eigenschappen die het Knooppunt heeft en ten dienste stelt aan het stelsel. Vandaar dat hieronder een overzicht wordt gegeven van de subcapabilities (in Archimate termen zijn dit voor een enabling capability tevens bedrijfsservices). Vanuit het Knooppunt is het dan belangrijk om dit uit te splitsen naar de aanbieder van API's, de afnemer van API's en de ondersteunende eigenschappen.

3.2 *Subcapabilities aanbieder*

Als eerste de subcapabilities die voorkomen in het aanbiedersperspectief.

#	Subcapabilities	Toelichting
1	Vertalen bericht	Deze service maakt vertalingen van berichten voor serviceaanbieders die hier gebruik van maken. De vertaling zorgt voor ontkoppeling tussen aanbieder en afnemer.
2	Identiteit aanmelden	Aanbieders en afnemers kunnen met deze service hun identiteit vastleggen. Deze identiteitsinformatie is onderdeel

		van de beveiligingsinformatie die binnen het stelsel gebruikt wordt voor authenticatie en autorisatie doeleinden.
3	Service beheer	Met deze service kunnen aanbieders zelf services aanmelden en wijzigen bij het Knooppunt. Aanbieders en afnemers geven hierbij aan welke functies van het Knooppunt zij daarbij willen gebruiken. Bijvoorbeeld authenticatie en autorisatie worden gebruikt waarbij aangegeven wordt welke rollen voor deze service geautoriseerd zijn. Met deze dienst kunnen afnemers zich aanmelden en afmelden voor het afnemen van services.
4	Toetsen toegang	Via deze service kunnen aanbieders, die een interne toetsingsprocedure hebben voor het verlenen van toegang tot hun service, deze koppelen aan de zelfbediening van het Knooppunt.
5	Aanbieden service	Met deze dienst worden services aangeboden op het Knooppunt. Dat wil zeggen het feitelijke berichtenverkeer loopt van aanbieder naar het Knooppunt.
6	Notificeren	Via deze service ontvangen[3] afnemers voor hun relevante informatie over wat er verandert aan de service die ze afnemen. Aanbieders ontvangen informatie over veranderingen in wie hun service afneemt.

3.3 *Subcapabilities afnemer*

In aanvulling hierop kent het afnemersperspectief de volgende capabilities.

#	Subcapabilities	Toelichting
7	Zoeken services	Via deze service kunnen afnemers zich oriënteren en informeren over de technische aspecten van services die in het stelsel beschikbaar zijn en waar zij op kunnen aansluiten. Voor semantische aspecten van services wordt een link naar de gegevenscatalogus aangeboden.
8	Afnemen service	Met deze dienst worden services afgenomen. Dat wil zeggen het aanroepen en gebruiken van een service. Hij realiseert de actieve verbinding tussen afnemer en het Knooppunt.

3.4 *Subcapabilities ondersteuning*

Voor de ondersteunende processen zijn er de volgende capabilities.

#	Subcapabilities	Toelichting
9	Ondersteuning gebruik	Met deze service worden aanbieders en afnemers ondersteund bij klachten en problemen rond het gebruik van het Knooppunt. Via ondersteunen gebruik wordt invulling

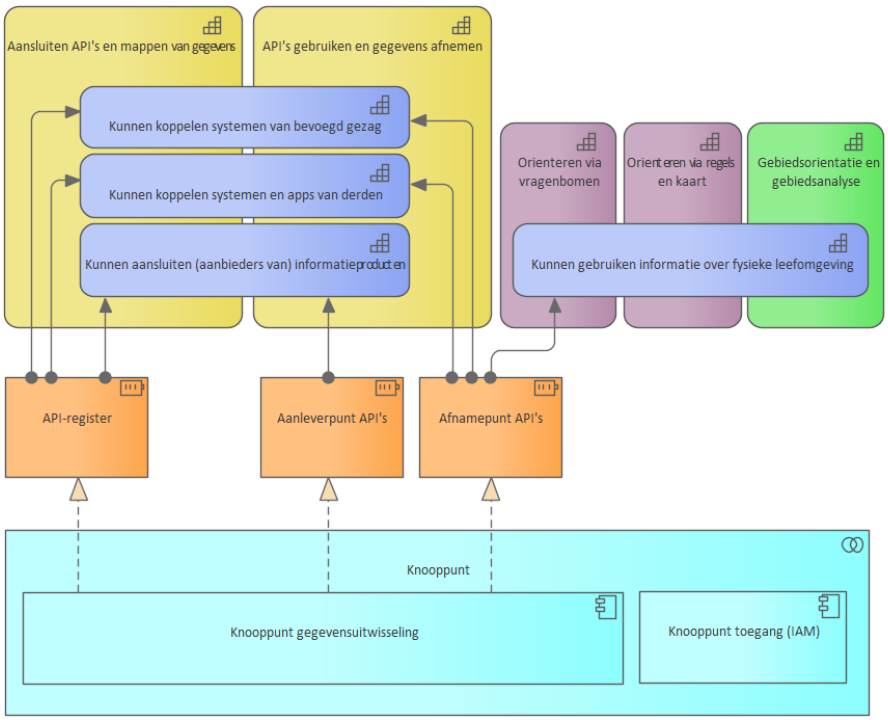
[3] Het kanaal voor notificaties is nog nader te bepalen en wordt uitgewerkt in de PSA. E-mail, berichtenbox en SMS zijn allemaal opties.

		gegeven aan vraagsturing[4]. De beheerorganisatie van het Knooppunt biedt via de serviceorganisatie van het stelsel (PR26) een 2e lijns helpdesk hiervoor.
10	Verantwoording berichtenverkeer	Met deze service kan achteraf verantwoording worden afgelegd wanneer een bericht is ontvangen of verstuurd inclusief de inhoud van het bericht. Ten behoeve van bezwaar, beroep en andere gevallen waarin juridisch moet worden aangetoond wat er heeft plaats gevonden op het gebied van berichtenverkeer.
11	Monitoren gebruik	Met deze service wordt bijgehouden wat het gebruik is van de services. Het gaat hierbij om het meten of aan de SLA voldaan wordt, maar ook het signaleren of grenswaarden overschreden worden zodat servicemanagement bij problemen proactief kan optreden.
12	Servicemanagement	Met deze service wordt operationeel en tactisch beheer uitgevoerd. Operationeel beheer zorgt ervoor dat het Knooppunt goed werkt. Tactisch beheer kijkt naar doorontwikkeling en geeft vorm aan verbetering van functionaliteit.

3.5 *Resources*

Deze paragraaf beschrijft de relevante resources voor deze GAS. Resources zijn mensen of systemen die worden toegewezen aan één of meer capabilities. Het gaat hierbij primair om resources die beschikbaar worden gesteld vanuit de landelijke voorziening(en). In dit geval worden ze gerealiseerd door het componentcluster Knooppunt Gegevensuitwisseling binnen DSO-LV.

[4] N.B. vraagsturing en de invulling van de serviceorganisatie zijn nog niet volledig uitgewerkt en kunnen nog veranderen.



Figuur 4 Resources

De resources zijn:

#	Resource	Toelichting
1	Aanleverpunt API's	De plaats waar aanbieders van services hun API's kunnen registreren zodanig dat zij deze API's aan afnemers ter beschikking kunnen stellen
2	Afnamepunt API's	De plaats van afnemers van API's kunnen zoeken in de beschikbare API's en vervolgens deze kunnen afnemen en gebruiken. Het zogenaamde vinden en verbinden.
3	API-Register	De registratie van alle beschikbare API's.

Hieronder wordt per resource een uitgebreide toelichting gegeven.

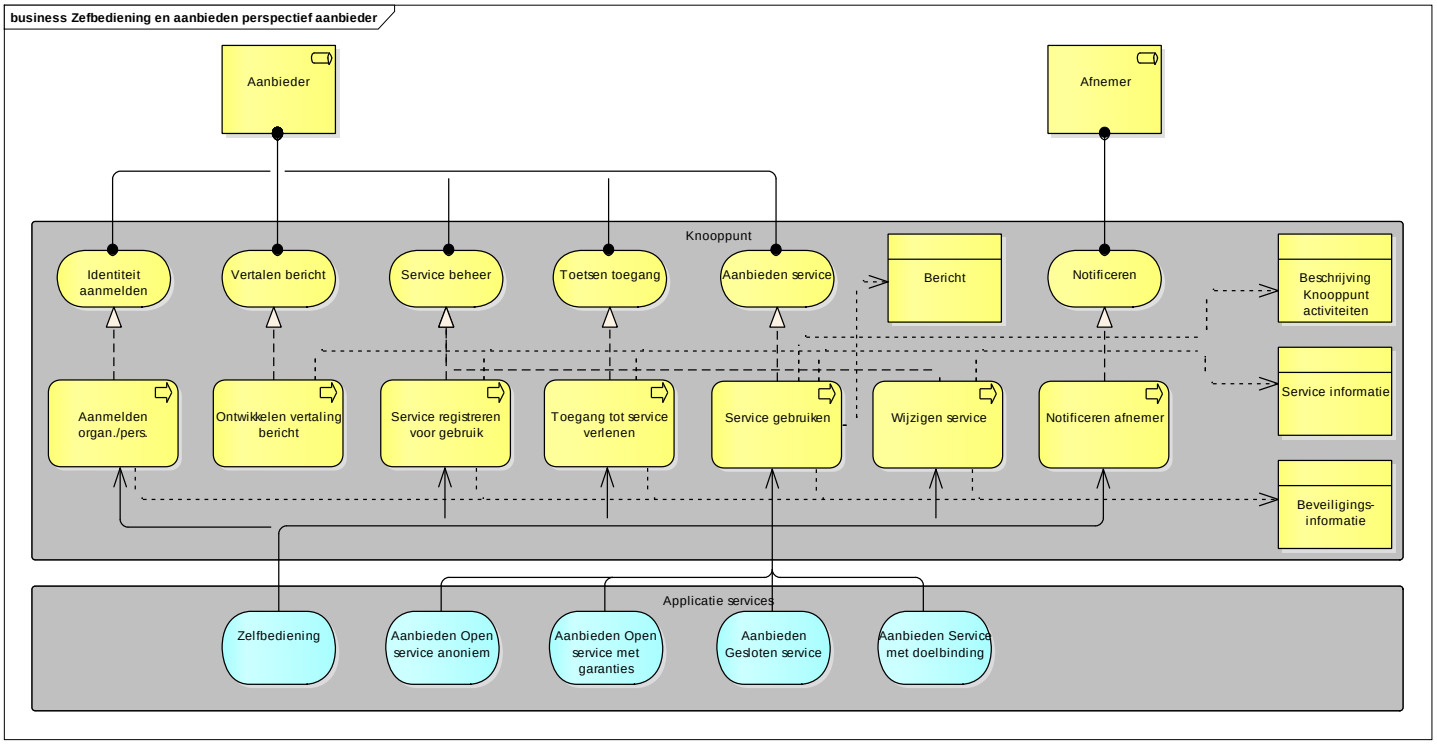
3.5.1 *Aanleverpunt API's: perspectief van de service aanbieder*

Deze view visualiseert het primaire proces voor het aanbieden van services op het Knooppunt vanuit het perspectief van de service aanbieder. De focus ligt op zelfbediening.

De interactie begint wanneer de aanbieder een service ontwikkelt. Bijvoorbeeld "aanvragen en melden" ontwikkelt een service voor communicatie met bevoegd gezag. Het Knooppunt kan hierin ondersteunen. Dit gebeurt door een vertaling te ontwikkelen die op het Knooppunt zorgt voor ontkoppeling met de afnemer. Het Knooppunt ondersteund "aanvragen en melden" en ontwikkelt in dit geval de vertaling tussen een vereenvoudigd interne service van "aanvragen en melden" en externe

service volgens de Digikoppeling standaard waarmee de communicatie vanaf het Knooppunt naar bevoegd gezag verloopt.

Is de service af dan registreert de aanbieder hem voor gebruik. Daarbij kan de aanbieder zijn eigen toegangseisen vastleggen voor het gebruik van de service. Bijvoorbeeld dat alleen bevoegd gezagen mogen aansluiten. Met de via zelfbediening vastgelegde service- en beveiligingsinformatie wordt de service vervolgens, zo veel als mogelijk geautomatiseerd, op het Knooppunt geconfigureerd zodat de service snel in gebruik genomen kan worden. Gebruik houdt in dat berichten worden uitgewisseld via het Knooppunt tussen aanbieder en afnemer. Wanneer een aanbieder gedurende de levenscyclus van een service (test, acceptatie, productie, end of life) iets aan een service wijzigt, meldt de aanbieder dit aan het Knooppunt.



Figuur 5. Primaire proces vanuit perspectief van de aanbieder

3.5.2 *Afnamepunt API's: perspectief van de service afnemer*

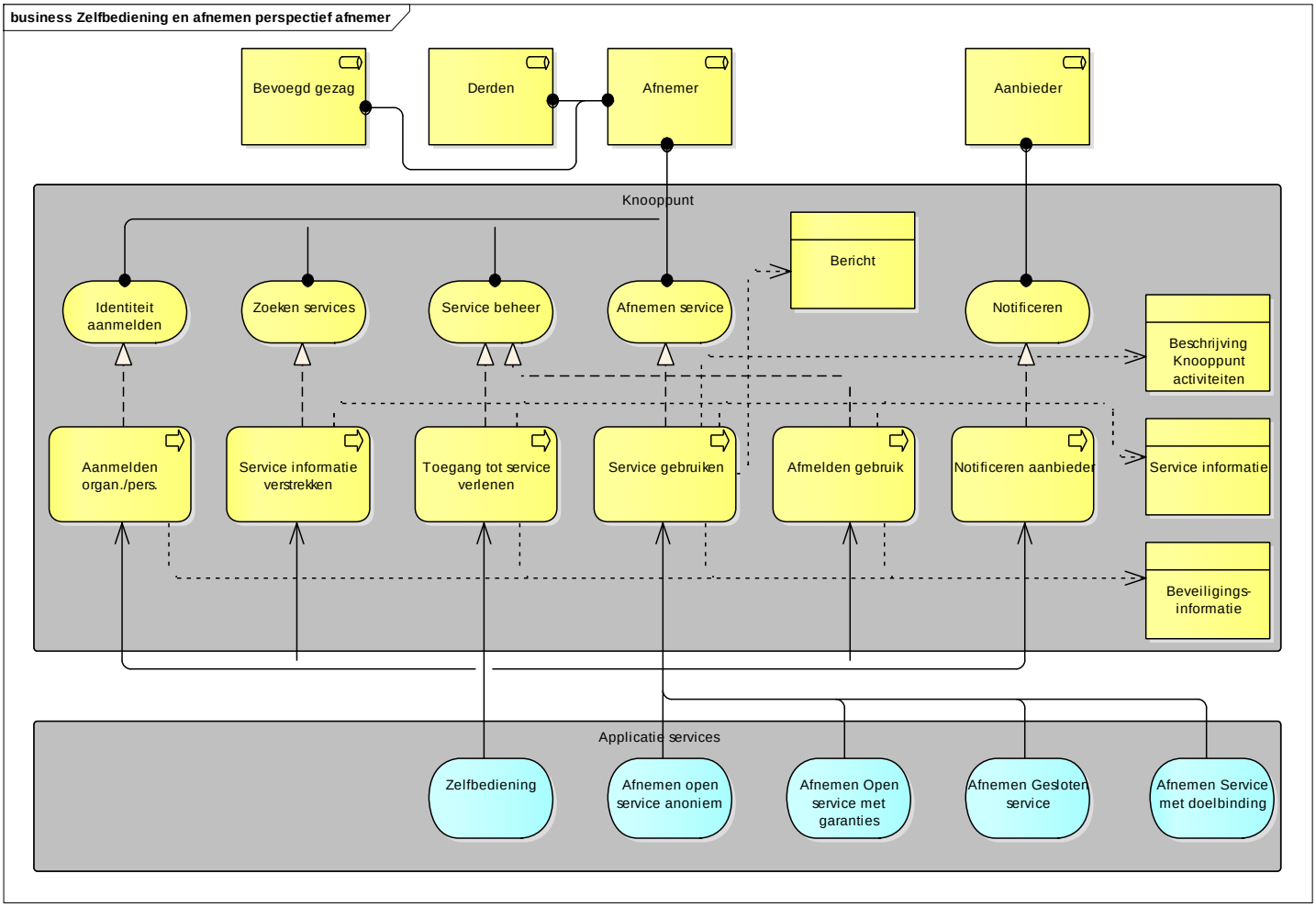
Deze view visualiseert het primaire proces voor het afnemen van services vanuit het perspectief van de service afnemer. Ook hier ligt de focus op zelfbediening.

Interactie met het Knooppunt begint al bij het ontwikkelen en configureren van de applicatie van de afnemer. Via het zelfbedieningsportaal kan hij relevante services met bijbehorende functionele documentatie en technische documenten vinden.

Wanneer zijn applicatie gereed is, registreert de afnemer zich voor het gebruiken van de gewenste services. Het Knooppunt wordt vervolgens zo veel als mogelijk automatisch geconfigureerd zodat het gebruik zo snel als mogelijk kan beginnen.

Gebruik houdt in dat berichten worden uitgewisseld via het Knooppunt tussen aanbieder en afnemer. Wanneer de afnemer stopt met het gebruiken van een service (wegens wijzigen of uit gebruik nemen van zijn applicatie) meldt hij zich af. Het Knooppunt past de configuratie automatisch hierop aan.

Figuur 6. Primaire proces uit perspectief van de afnemer

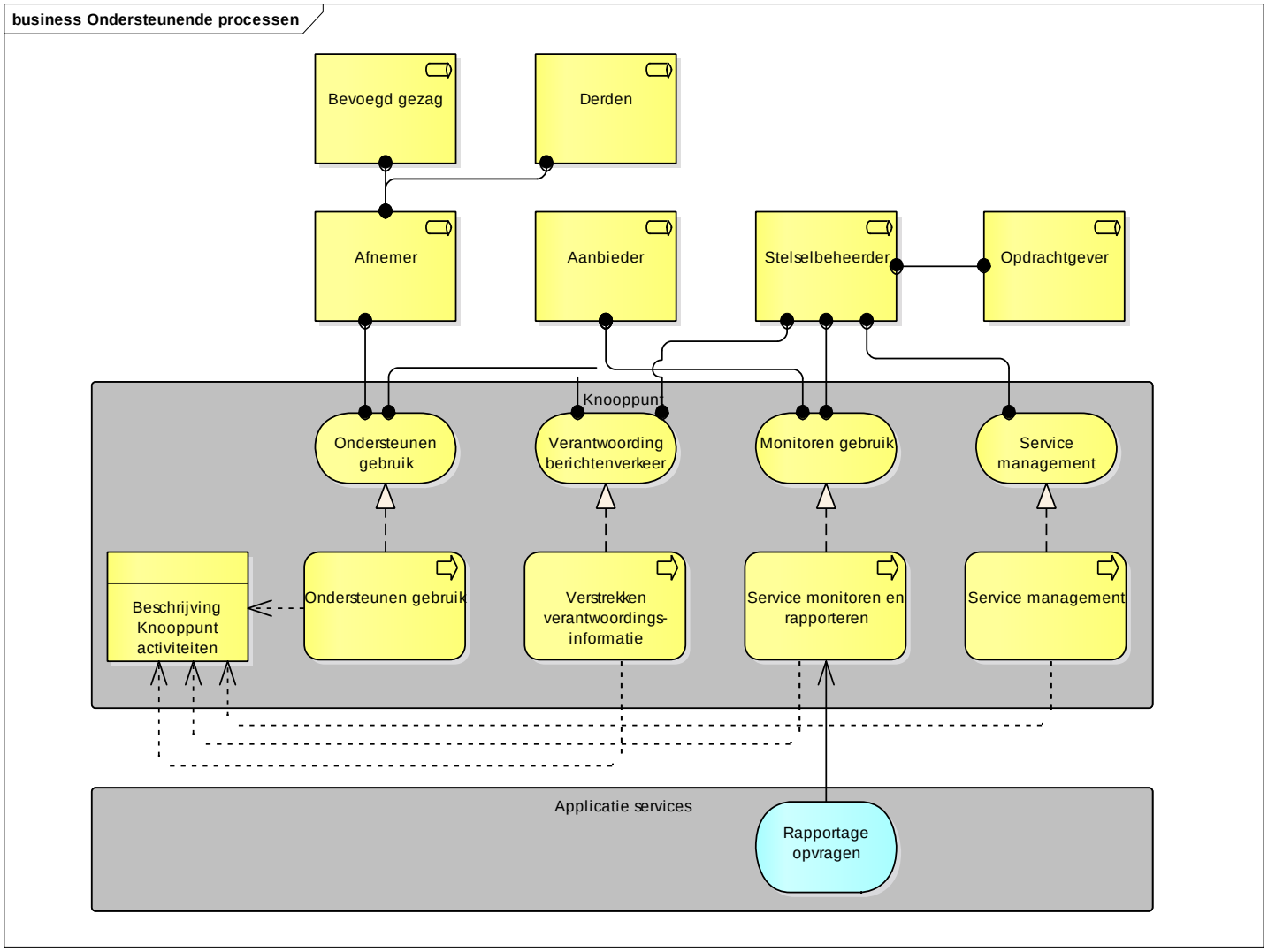


3.5.3 *API-register: De ondersteunende processen van het Knooppunt*

Deze view visualiseert de ondersteunende processen die het Knooppunt biedt naast het aanbieden en afnemen van services. Afnemers en aanbieders worden in hun gebruik ondersteund. Deze ondersteuning loopt via de serviceorganisatie van het stelsel. Ze kunnen storingen melden en vragen stellen bij problemen met aansluiten.

Aanbieders kunnen verantwoordingsinformatie opvragen over berichtenverkeer wanneer zij bijvoorbeeld betrokken zijn bij bezwaar en beroep procedures. Afnemers kunnen verantwoordingsinformatie opvragen via de stelselbeheerder. Naast verantwoordingsinformatie kunnen aanbieders ook het gebruik van services die ze

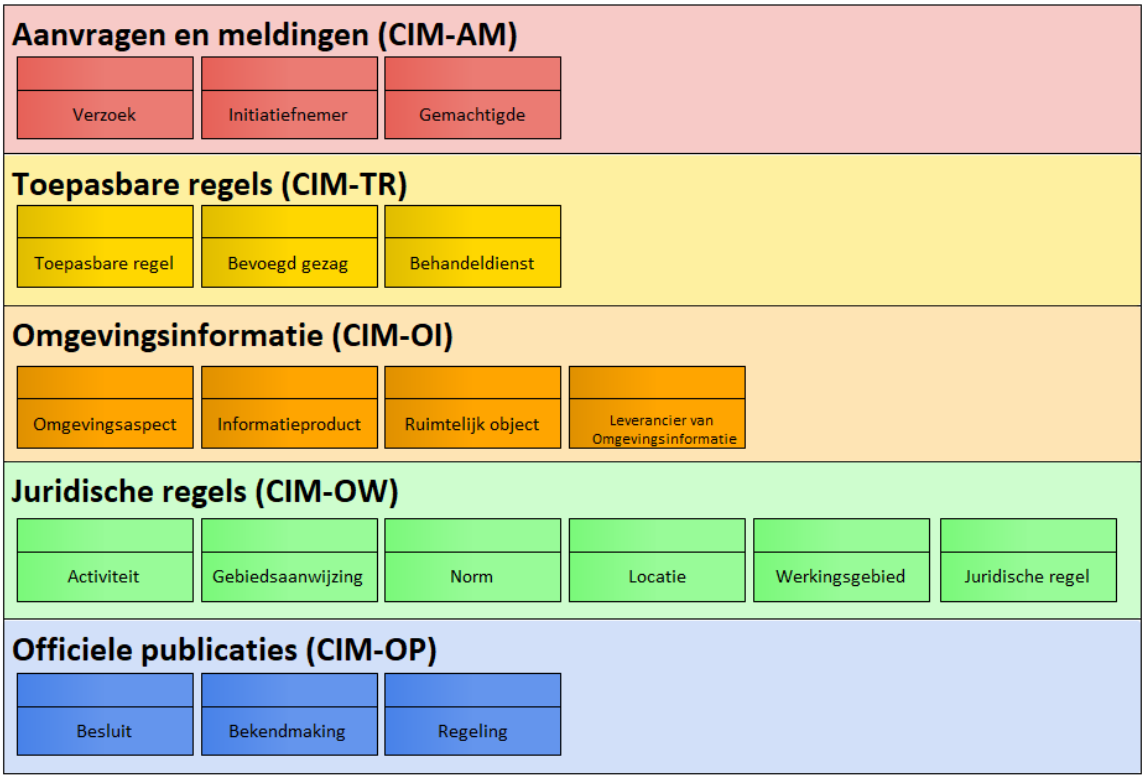
aanbieden monitoren. De stelselbeheerder kan dit gebruik ook monitoren ten behoeve van beleid. Tot slot wordt er servicemanagement uitgevoerd, dit zorgt ervoor dat de functionaliteiten van het Knooppunt goed werken en zorgt voor de verbetering van de capabilities en processen van het knooppunt. Waar nodig wordt afgestemd over de doorontwikkeling van functionaliteiten van het Knooppunt ter ondersteuning van deze verbeteringen.



Figuur 7 Ondersteunende processen

4 Informatie

In dit hoofdstuk wordt de Informatielaag beschreven van Knooppunt Gegevensuitwisseling, deze is bepalend voor de te kiezen oplossingen. In de OGAS is voor dit doel een globaal bedrijfsobjectenmodel (BOM) gepresenteerd. In onderstaand diagram is hierin met de rode omlijning weergegeven welke bedrijfsobjecten zich primair binnen het domein van Knooppunt Gegevensuitwisseling bevinden. Met de gele omlijning is aangegeven voor welke bedrijfsobjecten er sprake is van relaties/afhankelijkheden in aanliggende domeinen.



Figuur 8 Bedrijfsobjecten Model

De onderdelen in dit hoofdstuk worden in algemene zin beschreven in de OGAS. Deze GAS maakt een uitsnede op de onderdelen die van toepassingen zijn voor Knooppunt Gegevensuitwisseling.

4.1 *(bedrijfs)Objectenmodel*

Deze paragraaf beschrijft de (bedrijfs)objecten die van toepassingen zijn voor deze GAS.

#	Bedrijfsobject	Toelichting
	Geen	

De volgende interne Knooppunt (bedrijfs-)objecten worden in de ArchiMate views toegepast.

#	Interne bedrijfsobjecten	Toelichting
1	Beveiligingsinformatie	Informatie over identiteiten, machtigingen (=mandateringen) en autorisaties.
2	Service informatie	Technische beschrijving van services die afnemers nodig hebben om te koppelen en configuratie informatie waarmee het Knooppunt (automatisch) ingesteld kan worden om een service aan te bieden.
3	Beschrijving Knooppunt activiteiten	Dit omvat alle informatie rond het gebruik van services op het Knooppunt: gebruiksstatistieken, logging, auditing en berichtarchief informatie. Deze wordt vastgelegd met functionaliteit gerealiseerd door project Beveiliging (PR29).
4	Bericht	De informatie die daadwerkelijk wordt uitgewisseld tussen aanbieder en afnemer.

Deze instantiëren zich in een reeks dataobjecten/gegevens die hieronder worden genoemd.

4.2 *Gegevens*

Voor het Knooppunt is niet de semantiek van de gegevens uit het stelsel van belang maar de vorm. Het Knooppunt moet alle services die gegevens en functionaliteit leveren ontsluiten. Het Knooppunt moet dus ook om kunnen gaan met de vormen waarin aanbieders ze aanbieden en afnemers ze willen afnemen. Hierbij zijn de aanbieders van services gehouden aan de standaarden die voor het stelsel gelden.

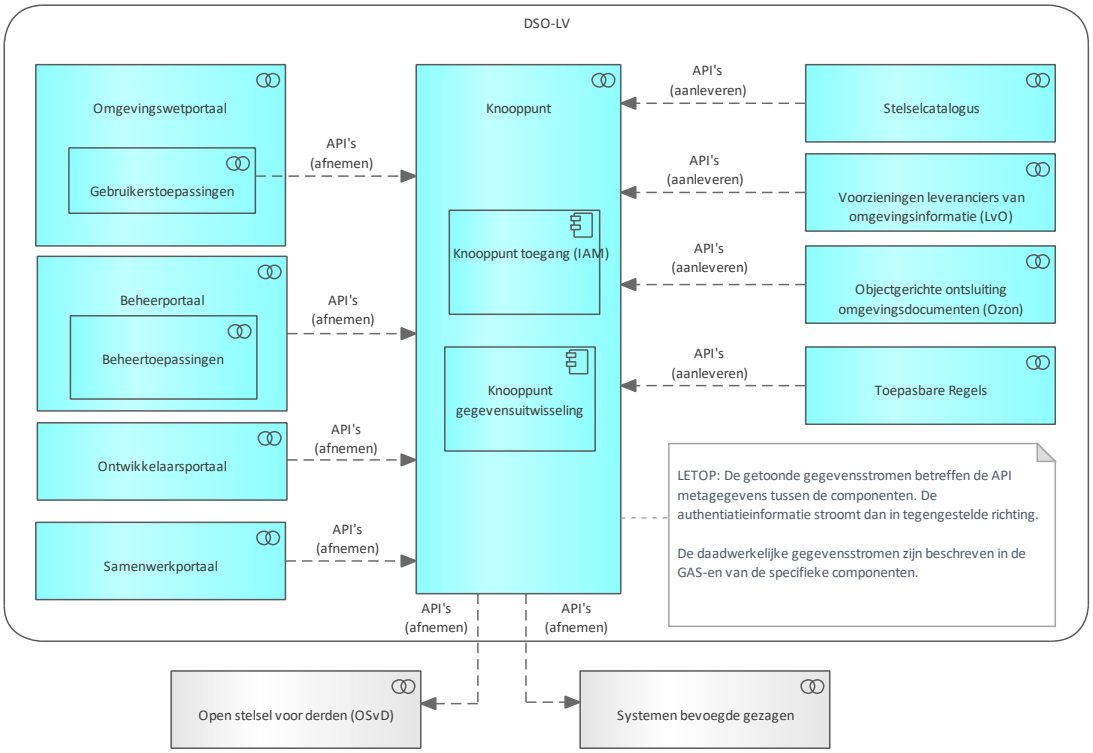
Het Knooppunt kent weinig gegevens van zichzelf, het is vooral een doorgeefluik voor gegevens en functionaliteiten van anderen.

#	Dataobject	Toelichting
1	Configuraties	Op basis van deze informatie kunnen het Integratieplatform en De Toegangspoort (automatisch) geconfigureerd worden en wordt het aanbieden en afnemen (automatisch) uitgerold in test en acceptatie omgevingen. Gegevens rondom het gebruik van services wordt door aanbieders zelf vastgelegd. Aanbieders leveren daarvoor een standaard beschrijving van de service met daarin: • Lifecycle stadium (ontwikkeling, test, acceptatie, productie, end of life) • Endpoint(s) • Technische documenten • Verwijzing (linked data) naar de Catalogus voor de semantiek • De te gebruiken Knooppuntfuncties Voor Stelsel componenten die gebruik maken van translatie/transformatie worden de bijbehorende vertaalregels ook vastgelegd in de configuraties.

		Afnemers geven aan: • Welke services ze afnemen • Hun endpoints, voor asynchrone uitwisselingen en tweerichtingsverkeer met aanbieders Op basis van deze informatie kunnen het Integratieplatform en De Toegangspoort zoveel mogelijk automatisch geconfigureerd worden en uitgerold in test en acceptatie omgevingen. In hoofdstuk beheer wordt toegelicht dat voor productie een handmatige controle vereist blijft vanwege toetsing op kwaliteit.
2	Autorisaties	Autorisatietabellen worden gebruikt om vast te leggen: • Wie heeft toegang tot welke services • Welke rollen welke autorisaties kennen • Welke gebruikers welke rollen bezitten
3	Log informatie	In de logs kunnen logging regels worden weggeschreven van het Knooppunt maar ook van andere applicaties binnen het DSO. Dit zorgt ervoor dat de serviceorganisatie van het stelsel eenvoudig diagnoses kan uitvoeren op problemen in de keten.
4	Archiveerbare berichten	Berichten waar later verantwoording over moet worden afgelegd worden gearchiveerd. Belangrijke eis is dat berichten die bij elkaar horen makkelijk aan elkaar te relateren zijn via een identificeerbaar kenmerk (bijvoorbeeld verzoeknummer) zodat doorzoeken voor verantwoording eenvoudig blijft.
5	Audit informatie	Voor het gebruik van services waarvoor audit verplichtingen gelden (zoals de BRP) dient informatie te worden opgeslagen over welke applicatie met welke gebruiker op welk moment welke interactie had.
6	Machtigingen informatie	Informatie die vastlegt welke identiteiten mogen acteren namens anderen en welke rollen zijn toegekend aan deze identiteiten.
7	Identiteiten	Informatie over de identiteit van een persoon of organisatie die met services van het stelsel communiceert. Bevat identificerende gegevens: voor organisaties (overheden/ bedrijven) het OIN, voor burgers het BSN, voor medewerkers van organisaties een niet tot persoonsinformatie te herleiden identificerend kenmerk. Gecombineerd met voorkeurs instellingen voor de gebruikersinterface van zelfbediening.

4.3 *Informatie-uitwisseling*

Deze paragraaf beschrijft de informatie-uitwisseling die van toepassing is op deze GAS. Het betreft hierbij de semantiek en de standaarden, niet de achterliggende techniek. Deze zal in hoofdstuk 5 worden toegelicht.



Figuur 9 Informatiestromen

#	Informatiestroom	Van	Naar	Toelichting
	API's (aanleveren)	Aanbieders	Knooppunt	Betreft de metagegevens
	API's (afnemen)	Knooppunt	Afnemers	Betreft de metagegevens
	API's (afnemen)	Knooppunt	OSvD/Bevoegd Gezagen	Betreft de metagegevens

De informatie-uitwisseling is verder opgesplitst in twee gedetailleerde views:

- Eén voor het proces Service gebruiken (en de ondersteunende processen).
- Eén voor het realiseren van de informatie-uitwisseling via zelfbediening.

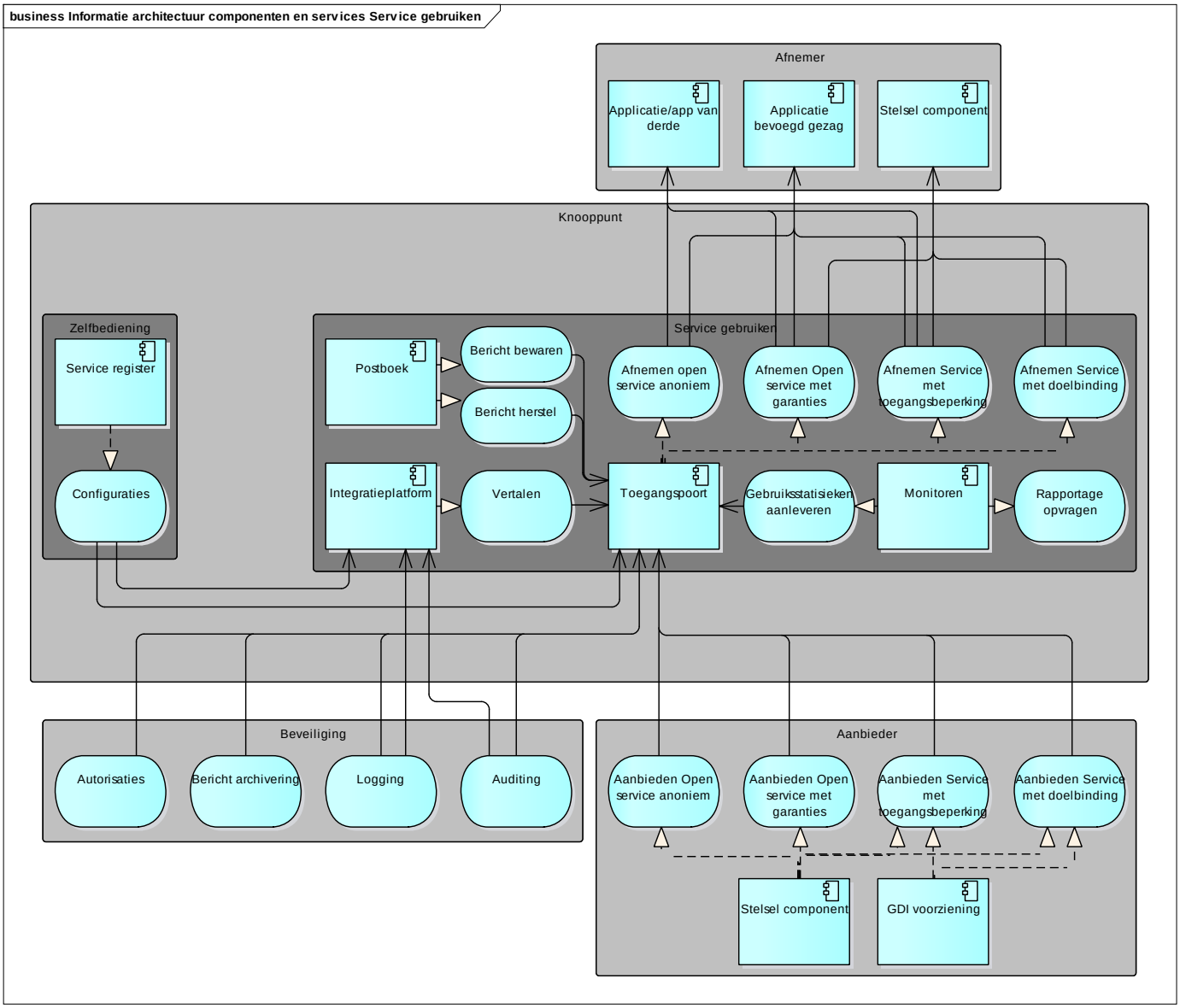
4.3.1 *Service gebruiken (en ondersteunende processen)*

Het Knooppunt vormt de kern van de informatie-uitwisseling van het DSO. Het benoemen van alle services die via het Knooppunt ontsloten worden leidt tot een onoverzichtelijk geheel. Vandaar dat alle afnemers en aanbieders tot abstracte afnemers en aanbieders zijn gedestilleerd.

Hetzelfde is gedaan met aan te bieden en af te nemen services. Hierin worden de 4 soorten services onderkent zoals beschreven in **Fout! Verwijzingsbron niet gevonden.**. Hoewel ze abstract zijn weergegeven, is hierover wel meer te vertellen. In het document achtergrond Knooppunt [Achtergrond] is dit uitgebreid toegelicht.

Het gaat in op afnemers- en aanleverkoppelvlakken en standaarden (linked data, geo informatie, REST, Digikoppeling) die een rol spelen.

Onderstaand overzicht beschrijft in detail de specifieke informatie-uitwisseling rondom de werking van het Knooppunt zelf. Centraal staat Toegangspoort, waar alle berichten langs lopen. Voor een aantal uitwisselingen wordt deze ondersteund door het Integratieplatform die translatie/transformatie (waaronder Digikoppeling) afhandelt. Deze twee componenten worden zo veel mogelijk automatisch geconfigureerd op basis van informatie die via zelfbediening in het serviceregister is vastgelegd. Functionaliteit rondom beveiliging als ook logging, auditing en berichtarchivering wordt met verschillende services van de bouwblokken die het project Beveiliging levert, gerealiseerd.



Figuur 10. Informatie uitwisseling service gebruiken

In bovenstaand diagram zijn alle componenten van het Knooppunt zelf benoemd, hier worden ze aangevuld met externe componenten die in de informatie-uitwisseling een rol spelen.

#	Componenten	Toelichting
10	Applicatie bevoegd gezag	Het bevoegd gezag neemt services van het stelsel af voor het uitvoeren van haar taak. Dit kunnen alle type services van het stelsel zijn.
11	Applicatie/app van derde	De applicatie van een derde handelt namens een burger, bedrijf of overheid. Hij neemt alleen services af en heeft daarbij (waar nodig) de rollen waarvoor een burger, bedrijf of overheid hem machtigt.
12	Stelsel component	Dit is een component gerealiseerd door één van de applicaties binnen het DSO: Toepasbare regels, Aanvragen en melden, Catalogus, Samenwerken, Gebruikerstoepassingen en Informatiehuis. Applicaties binnen het DSO kunnen services aanbieden en afnemen. Applicaties binnen het DSO kunnen gebruik maken van functies gerealiseerd door het Integratieplatform
13	GDI voorziening	GDI voorzieningen worden op het Knooppunt ontsloten, vaak met een vereenvoudigde service voor gebruik door Stelsel componenten.

De services die door deze componenten worden aangeboden:

#	Service gebruiken	Toelichting
1	Autorisaties	Toegang controleren realiseert een service waarmee autorisaties kunnen worden vastgelegd en bevraagd. De Toegangspoort maakt hier gebruik van bij het autoriseren van afnemers op grofmazig niveau (wel of geen toegang tot de service). De API Manager gebruikt deze service om autorisaties en machtigingen (=mandateringen) die voortkomen uit Zelfbediening vast te leggen.
2	Berichtarchivering	Via deze service kunnen berichten worden vastgelegd in het berichtarchivering component.
3	Logging	Via deze service wordt logging van het Knooppunt vastgelegd en opgevraagd in de logging component.
4	Auditing	Via deze service wordt audit informatie over het gebruik van services met doelbinding vastgelegd.
5	Aanbieden Open service anoniem	Een door een aanbieder aangeboden open service.
6	Aanbieden Open service met garanties	Een door een aanbieder aangeboden open service met garanties.
7	Aanbieden Service met toegangsbeperking	Een door een aanbieder aangeboden service met toegangsbeperking.
8	Aanbieden Service met doelbinding	Een door een aanbieder aangeboden service met doelbinding.

De services die gerealiseerd worden:

#	Service realiseren	Toegang	Toelichting
1	Configuraties	Knooppunt intern	Het service register realiseert een service waarmee De Toegangspoort en Integratieplatform componenten zichzelf kunnen configureren. Het Integratieplatform en De Toegangspoort halen bij deze service de configuratie informatie op voor het realiseren van services. Zelfbediening legt via deze service de configuraties vast die aanbieder en afnemer hebben ingesteld.
2	Vertalen	Knooppunt intern	Integratieplatform component realiseert deze service voor het aanbieden en afnemen van

			services waarop zij validaties, transformaties en/of translaties uitvoert. Het Integratieplatform handelt met vertalen ook het Digikoppeling protocol af. Dit houdt in het vertalen (translatie) van een simpele service naar Digikoppeling t.b.v. stelselcomponenten.
3	Gebruiksstatistieken aanleveren	Knooppunt intern	Via deze service levert De Toegangspoort informatie aan over het gebruik van services op het Knooppunt.
4	Rapportage opvragen	DSO	Deze service wordt als een webportaal geïmplementeerd. Gebruikers kunnen hierin zelf hun rapportages opvragen.
5	Bericht bewaren	Knooppunt intern	Via deze service worden alle berichten die via het knooppunt lopen tijdelijk opgeslagen in het Postboek.
6	Bericht herstellen	Knooppunt intern	Via deze service kan een beheerder met behulp van een gebruikersinterface berichten uit het postboek herstellen (opnieuw versturen).
5	Aanbieden Open service anoniem	DSO/Open	Via deze service nemen afnemers open data af zonder authenticatie en beschikbaarheidsgaranties, zie ook toelichting hieronder.
6	Aanbieden Open service met garanties	DSO/Open	Via deze service nemen afnemers open data af met authenticatie en garanties, zie ook toelichting hieronder.
7	Aanbieden Service met toegangsbeperking	DSO/Open	Via deze service nemen afnemers services af waar zij vanuit hun rol toegang toe hebben. Met authenticatie en SLA, zie ook toelichting hieronder.
8	Aanbieden Service met doelbinding	DSO	Via deze service nemen afnemers services af die doelbinding vereisen. Met authenticatie en SLA, zie ook toelichting hieronder.

4.3.2 *Zelfbediening*

De API Manager applicatiecomponent biedt een zelfbedieningsportaal aan. Dit is een gebruikerstoepassing. Ter illustratie: vanuit het perspectief van de gebruiker kan het als volgt werken. Na inloggen met DigiD of eHerkenning wordt aan de hand van de vastgestelde identiteit bepaald met welke rollen een gebruiker mag handelen. Afhankelijk van de rol zijn andere functionaliteiten beschikbaar.

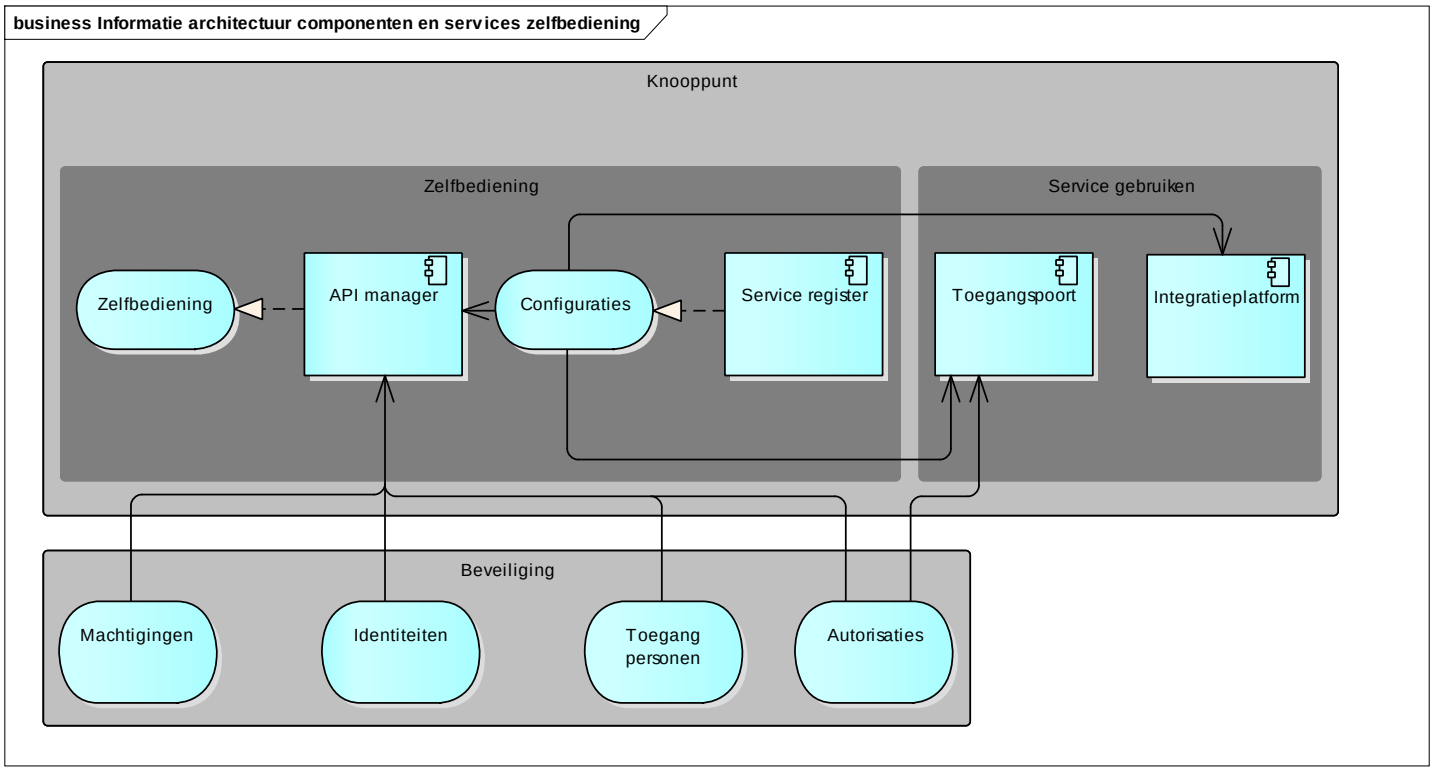
Bijvoorbeeld: Een medewerker van een overheid die een stelselcomponent ontwikkeld logt in met eHerkenning, hij handelt altijd namens de overheid. De medewerker heeft (via eHerkenning) de rollen afnemer en aanbieder meegekregen.

- Als aanbieder kan hij een service van zijn overheidsorganisatie op het Knooppunt aanmelden en instellen welke functies ingeschakeld moeten worden voor de service.
- Als afnemer kan hij in de stelselcatalogus zoeken welke gegevens en services hij wil afnemen. In de stelselcatalogus vindt hij een link naar de API manager. Daar kan hij de functionele en technische documentatie inzien.
- Als afnemer kan hij in de API manager zoeken welke services hij mag afnemen. Hij kan de functionele en technische documentatie inzien en vindt bij een

service een link naar de Catalogus voor informatie over de gegevens die de service levert.
- Als afnemer kan hij in de API manager systemen van zijn overheid aanmelden en registreren welke services ze af willen nemen.

Een ander voorbeeld: een burger logt in met DigiD, hij handelt namens zichzelf en kan alleen de rol afnemer hebben. In het zelfbedieningsportaal kan hij:
- Als Afnemer een app op zijn mobiele telefoon autoriseren om namens hem te handelen.

Technisch werkt het als volgt. De invoer van de afnemer en aanbieder wordt vastgelegd. Voor technische informatie over services gebeurt dit in het service register. Voor informatie rondom beveiliging (autorisaties en machtigingen) wordt dit vastgelegd met de services die de bouwblokken van Beveiliging bieden. Het inloggen op het portaal wordt gerealiseerd met de Toegang personen service van Beveiliging. De gebruikers gegevens en voorkeuren voor de website worden via de Identiteiten service van Beveiliging vastgelegd en opgevraagd.



Figuur 11. Informatie-uitwisseling Zelfbediening

In **Fout! Verwijzingsbron niet gevonden.** zijn alle componenten van het Knooppunt uit bovenstaande view al beschreven.

In 4.3.1 zijn een aantal services ook al beschreven. De aanvullende services worden in onderstaande tabellen behandeld.

De services die door deze componenten worden aangeboden:

#	Service gebruiken	Toelichting

9	Machtigingen	De machtigingen component realiseert een service waarmee machtigingen (=mandateringen) kunnen worden vastgelegd en geraadpleegd.
10	Identiteiten	De componenten organisatiebeheer en gebruikersbeheer bieden een service waarmee identiteiten kunnen worden vastgelegd en opgevraagd.
11	Toegang personen	Vanuit het Toegang personen onderdeel van Toegang controle wordt een generieke service gerealiseerd waarmee personen kunnen worden geauthenticeerd (met naar keuze DigiD of eHerkenning en in de toekomst Idensys).

De services die gerealiseerd worden:

#	Service realiseren	Toegang	Toelichting
9	Zelfbediening	DSO/Open	Deze service ontsluit de hierboven omschreven functionaliteit naar de gebruiker en wordt geïmplementeerd als webportaal. De webportaal wordt bij voorkeur vanuit het perspectief van de gebruiker geïntegreerd in het Omgevingsloket aangeboden en minimaal aangepast aan de Look & Feel opgeleverd door PR11.

4.4 *Standaarden*

In deze paragraaf worden de aanvullingen/uitzonderingen op standaarden (benoemd in de OGAS) beschreven die van toepassing zijn voor deze GAS.

Voor het Knooppunt zijn er een groot aantal standaarden van de PTOLU lijst relevant die ook in de OGAS zijn opgenomen. Specifiek voor Knooppunt Gegevensuitwisseling worden onderstaande hier uitgelicht:

Naam	Omschrijving	Bron	Beherende organisatie	Versie	Informatie
Digikoppeling standaarden (ebMS)	Digikoppeling, versie 2.0, bestaat uit koppelvlakstandaarden, die logistieke afspraken bevatten voor berichtenuitwisseling tussen overheden waaronder ebMS: voor meldingen tussen informatiesystemen	Logius	Logius	2.0	Verplichte ('pas toe of leg uit') open standaard. Forum Standaardisatie / In de toekomst mogelijk via AmvB op grond van Wet digitale overheid
HTTPS	Transportprotocol. Zorgt voor beveiligde communicatie tussen een webclient zoals een webbrowser en een webserver	IETF	IETF	RFC 2818	Verplichte ('pas toe of leg uit') open standaard. Forum Standaardisatie
Open API Specification	The goal of The OpenAPI Specification is to define a standard, language-agnostic interface to REST APIs which allows both humans and computers to disco ver and understand the capabilities of the service without access to source code, documentation, or through network traffic inspection.	Open API Initiative	Open API Initiative	3.0	Verplichte ('pas toe of leg uit') open standaard. Forum Standaardisatie

PKIoverheid	Voorgeschreven standaard voor PKI certificaten binnen Nederlandse Overheid. Voorschrift volgt o.a. uit diverse andere standaarden zoals DigiKoppeling en aansluitvoorwaarden van GDI.	Logius	Logius	4.4	Het PvE PKI overheid is niet statisch. Als standaard geldt steeds de meest recente versie plus de gepubliceerde wijzigingen, zie https://www.logius.nl/ondersteuning/pkioverheid/aansluiten-als-tsp/programma-van-eisen/actuele-wijzigingen/

Daarnaast is er nog een reeks JSON standaarden die van betekenis bij de toepassing van JSON/REST als communicatieprotocol. Zie hiervoor de OGAS waar deze zijn opgesomd.

5 Applicatie

In dit hoofdstuk wordt de Applicatielaag beschreven van Knooppunt Gegevensuitwisseling, deze is bepalend voor de te kiezen oplossingen.

Afhankelijk van de aard van de service zijn er op informatieniveau verschillende functies beschikbaar om de inspanning van de service aanbieder te beperken (verkleinen van de beheer footprint) en integraal beheer van het stelsel te optimaliseren.

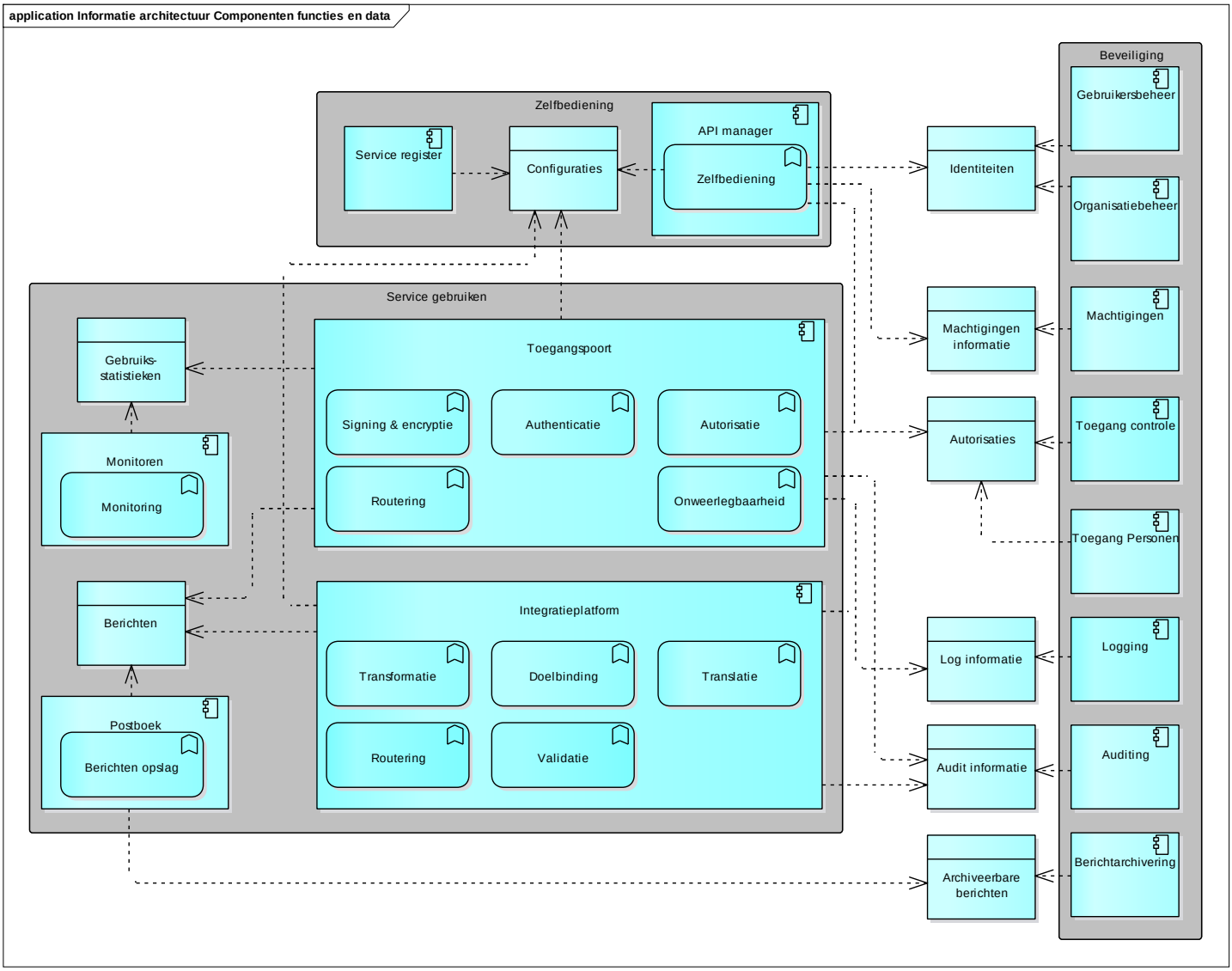
De functies Zelfbediening, Routering en Monitoring zijn voor elke service ingeschakeld. Routering en Monitoring worden echt bij iedere uitwisseling gebruikt. Zelfbediening wordt gebruikt voor het zoveel mogelijk automatiseren van herhalende beheerprocessen. Zelfbediening wordt dus niet bij ieder bericht toegepast, maar wel altijd bij in- en uitgebruik nemen van services. De overige functies zijn optioneel en worden door de service aanbieder alleen ingeschakeld wanneer de aard van de service dit vereist.

5.1 *Applicatie componenten*

Deze paragraaf beschrijft de applicatiecomponenten die van toepassingen zijn op deze GAS.

#	Componenten	Toelichting
1	Toegang controle	Toegang controle is een bouwblok dat wordt ingericht door Beveiliging. Deze wordt gebruikt om autorisaties vast te leggen, en te bevragen. Ook kunnen waar nodig machtigingen geraadpleegd worden. Bijvoorbeeld of een app dat ontwikkeld is door een derde is gemachtigd om namens een bij het DSO bekende gebruiker te handelen. Wanneer gevraagd wordt of de app geautoriseerd is neemt Toegang controle op deze machtiging mee in de autorisatie beslissing.
2	Machtigingen	Machtigingen is een bouwblok dat ingericht wordt door Beveiliging. Hierin kunnen machtigingen worden vastgelegd. Voor het Knooppunt worden twee soorten machtigingen vastgelegd. Apps van derden die namens een identiteit (persoon of organisatie) mogen handelen en mandateringen.
3	Toegangspoort	De Toegangspoort vormt de basis van het Knooppunt en is een te leveren bouwblok. Het virtualiseert de services van aanbieders en biedt ze centraal via één server adres met één domeinnaam aan. De Toegangspoort wordt gebruikt door alle afnemers en aanbieders bij het uitwisselen van berichten. De Toegangspoort implementeert de functies Authenticatie, Autorisatie, Signing & encryptie, Onweerlegbaarheid en Routering. Voor Autorisaties wordt bouwblok Toegang controle geraadpleegd.
4	API Manager	Dit is de centrale component voor zelfbediening en een te leveren bouwblok. Het biedt afnemers en aanbieders een webinterface om het gebruik van services te registreren en configureren. De API Manager is afhankelijk van het service register voor het vastleggen en opvragen van configuratie informatie. Daarnaast is de API Manager afhankelijk van het bouwblok Toegang controle voor het vastleggen van autorisaties en maakt het gebruik van Toegang personen voor authenticatie van gebruikers op de webinterface.

5	Service register	Legt technische configuratie informatie rondom het gebruik van services per service vast ten behoeve van de API manager. Het is een te leveren bouwblok. Let op dit is dus niet de catalogus met semantische informatie.
6	Logging	De logging component verzorgt de opslag van logfiles, maar faciliteert ook het opvragen van deze gegevens en het doen van analyse op deze gegevens. Logging is een bouwblok dat geleverd wordt door beveiliging.
7	Berichtarchivering	Berichtarchivering biedt een centrale plek voor de opslag van te archiveren berichten en faciliteert ook het opvragen van deze berichten ten behoeve van verantwoording. Berichtarchivering is een door Beveiliging te leveren bouwblok.
8	Auditing	Auditing biedt een centrale plek voor de opslag van auditinformatie en faciliteert ook het opvragen van deze informatie ten behoeve van verantwoording. Auditing implementeert is een door Beveiliging te leveren bouwblok.
9	Integratieplatform	Het integratieplatform handelt transformaties, translaties, Routering en doelbinding af. Het is een op te leveren bouwblok. ***Zie paragraaf 5.1.1***
10	Postboek	Dit component raadpleegt gearchiveerde berichten. Het wordt geraadpleegd voor analyses over wat er fout is gegaan met het berichtenverkeer. Het postboek biedt daarnaast mogelijkheden voor het herstellen (opnieuw versturen) van berichten waarmee iets fout is gegaan.
11	Monitoren	Met het monitoren component wordt het gebruik van service op het Knooppunt geregistreerd, daarnaast biedt het een interface waarmee rapportages over het gebruik van services op te vragen zijn.
12	Gebruikersbeheer	Gebruikersbeheer biedt een centrale plek waar identiteitsgegevens als ook de voorkeuren van gebruikers in webinterfaces als zelfbediening kunnen worden opgeslagen. Gebruikersbeheer is een door Beveiliging te leveren bouwblok.
13	Organisatiebeheer	Organisatiebeheer biedt een centrale plek waar gegevens over organisaties zoals identiteitsgegevens kunnen worden opgeslagen. Organisatiebeheer is een door Beveiliging te leveren bouwblok.
14	Toegang Personen	Toegang personen is een generieke voorziening waarmee personen zich kunnen authenticeren. Een persoon kan daarbij kiezen uit DigiD, eHerkenning of in de toekomst Idensys.



Figuur 12 Informatie uitwisseling applicatie componenten

5.1.1 *Uitgebreide toelichting Integratieplatform*

Het Integratieplatform realiseert functies die worden gebruikt door stelselcomponenten uit de Overall GAS (OGAS): Aanvragen en Melden, Toepasbare regels, Samenwerken, Catalogus, Gebruikerstoepassingen en Aansluitpunt Informatieproducten. Deze stelselcomponenten kunnen gebruik maken van de transformatie en translatie functionaliteit die een integratieplatform biedt om te vertalen tussen berichtformaten en inhoudelijke formaten. De transformatie wordt op het Knooppunt als een service aangeboden. Die service is dan toegankelijk voor iedere interne afnemer die de juiste rol heeft en (indien van toepassing) zijn of haar doelbinding kan aantonen.

Beoogde transformaties zijn het aanbieden van vereenvoudigde services op basisregistraties. Basisregistraties zijn breed opgezet om een zo groot mogelijke doelgroep te bedienen. Het gebruik van services van deze basisregistraties vraagt vaak hele specifieke kennis. Afnemers hebben een specifieke informatiebehoefte. Een wijziging van een service verandert meestal niets aan de informatie die een afnemer nodig heeft en vergt vanuit afnemers perspectief onnodige aanpassingen. De afnemer wil een stabiele service met alleen de informatie die hij nodig heeft, die niet onnodig wijzigt en die met minimale kennis te gebruiken is. Dit verbetert de stabiliteit van services en maakt deze eenvoudiger in gebruik. Hierdoor merken afnemers niets van wijzigingen bij externe services.

Het Integratieplatform handelt het Digikoppeling protocol af. Het gaat hierbij om de translatie van een vereenvoudigd bericht protocol naar Digikoppeling, zodat niet alle stelselcomponenten uit de OGAS zelf Digikoppeling hoeven te implementeren. Daarnaast handelt het Integratieplatform ook het routeren van Digikoppeling berichten af.

Verder handelt het Integratieplatform de technische aspecten van doelbinding af, hiermee kan op een vereenvoudigde manier worden aangesloten op services die doelbinding vereisen zoals de BRP. Doelbinding betekent dat iemand (persoon of organisatie) slechts dan, en alleen dan, informatie mag vragen, opslaan, gebruiken, delen wanneer dat een (geautoriseerd) heel specifiek en eigenlijk doel dient. De informatie is ook beperkt tot die informatie die nodig is voor het doel en niet meer. Dit wordt opgeslagen in de autorisatie informatie en door het integratie platform gebruikt bij de uitvoering van bevragingen. Het bevragen van deze (basis)registraties is namelijk alleen mogelijk als hier expliciet toestemming voor is. Bij het afnemen van een service met doelbinding wordt expliciet gecheckt op de aanwezigheid van deze toestemming. Het verkrijgen van deze toestemming wordt ook wel functioneel aansluiten genoemd. Voor het functioneel aansluiten wordt vanuit de beheer organisatie ondersteuning geboden indien nodig.

Stelselcomponenten kunnen met het in de business architectuur beschreven proces een verzoek indienen om een transformatie/translatie te realiseren. Het is hierbij belangrijk om op te merken dat het Knooppunt geen businesslogica bevat. Translaties en transformaties hebben dus alleen te maken met de vorm van berichten. Hooguit wordt informatie weggelaten (zoals bij basisregistraties). Er wordt echter niet op basis van kennis van de business informatie geaggregeerd, samengevoegd of op een andere manier informatie aangepast.

5.2 *Applicatiefuncties*

De volgende applicatiefuncties worden middels de hierboven beschreven applicatie componenten geleverd.

Figuur 13. Applicatiecomponenten en -functies

#	Applicatiefunctie	Toelichting
1	Authenticatie	Het betrouwbaar vaststellen van de identiteit van een afnemer of aanbieder. Op systeemniveau met PKIoverheid certificaten of OAuth. OAuth voor het authenticatie van apps van derden. PKIOverheid voor overheidssystemen. OAuth of SAML voor het doorgeven van de identiteit van eindgebruikers. Zie hoofdstuk beveiliging voor meer details. Type: optioneel
2	Autorisatie	Toegang verlenen tot beveiligde services op basis van geslaagde authenticatie. Het Knooppunt autoriseert toegang tot de service. De service zelf autoriseert toegang op dataniveau door gegevens te filteren zodat alleen geautoriseerde gegevens toegankelijk zijn. Dit is mogelijk doordat het Knooppunt de identiteit meestuurt ("identity propagation"). Type: optioneel
3	Doelbinding	Bij het aansluiten op (basis)registraties die doelbinding vereisen de technische aansluiting vereenvoudigen. Bijvoorbeeld voor de BRP het standaard DSO authenticatiemiddel van de afnemer vertalen naar het wachtwoord voor autorisatie van die afnemer dat BRP vereist. Daarnaast voor de BRP ook het actueel houden van dit wachtwoord wanneer het aangepast moet worden. Type: optioneel
4	Monitoring	Het verzamelen van informatie over het gebruik van services. Aantallen requests, responsetijden etc. Voor het genereren van rapportages, bijvoorbeeld om te rapporteren of SLAs worden gehaald en proactief te handelen bij problemen bij het overschrijden van drempelwaarden. Type: altijd aan
5	Onweerlegbaarheid	Ten behoeve van processen met rechtsgevolgen kunnen bewijzen dat een bericht is afgeleverd of ontvangen en dat de inhoud van het bericht juist en intact was bij aflevering. Maakt gebruik van de bouwblokken auditing en berichtarchivering . Bij het vastleggen van informatie in de bouwblokken van beveiliging ten behoeve van onweerlegbaarheid wordt gebruik gemaakt van technieken als hashing of signing van deze informatie welke onweerlegbaarheid mogelijk maken. Zie paragraaf 8.4 voor meer uitleg. Type: optioneel
6	Berichten opslag	Het (tijdelijk) opslaan van volledige berichten. Wordt gebruikt voor oplossen van problemen in het functioneren van services. Zowel voor analyse (inzien berichten) als herstel (herinjectie berichten). Zie ook hoofdstuk beheer. Type: Altijd aan

#	Applicatiefunctie	Toelichting
7	Routering	Een bericht van aanbieder naar afnemer transporteren en vice versa. Het Knooppunt kent alle service endpoints van aanbieders en afnemers waar verbindingen mee worden gelegd. Afnemers en aanbieders koppelen technisch één keer met het Knooppunt en kunnen dan communiceren met alle aangesloten aanbieders en afnemers. Dit leidt tot een reductie van complexiteit in het aantal te beheren verbindingen.[5] Type: altijd aan
8	Signing & Encryptie	Het versleutelen van de transportlaag en het versleutelen en/of ondertekenen van berichtinhoud. Type: optioneel
9	Transformatie	Het veranderen van het formaat van de inhoud van berichten, bijvoorbeeld een vereenvoudigde interne service met vereenvoudigde vraag- en antwoordbericht. Deze bevatten alleen de noodzakelijk informatie om bijvoorbeeld een basisregistratie te kunnen bevragen en geeft alleen de relevante informatie terug aan de aanroeper. Type: optioneel
10	Translatie	Het vertalen van het ene transport protocol naar het andere. Bijvoorbeeld SOAP naar REST of WS-RM naar ebMS. Type: optioneel
11	Validatie	Vaststellen of een bericht (envelop en inhoud) voldoet aan de afgesproken standaard(en) en eventueel aanvullende afspraken. Type: optioneel
12	Zelfbediening	Zelfbediening wordt gerealiseerd met de API Manager applicatie-component. Hiermee worden herhalende beheerhandelingen zoveel als mogelijk geautomatiseerd. Type: altijd aan

5.3 *Herbruikbare bouwblokken*

In deze paragraaf worden de aanvullingen/uitzonderingen op herbruikbare bouwblokken beschreven, benoemd in de OGAS.

Als enabling capability is het Knooppunt zelf in zijn geheel een bouwblok waarbij de subcapabilities zoals eerder beschreven eigenschappen zijn die meestal zelfstandig gebruikt kunnen worden.

De volgende bouwblokken worden opgeleverd als herbruikbaar DSO bouwblok:

[5] N.B. Routering komt voor in de toegangspoort en in het integratieplatform. In de eerste wordt routering op de transportlaag gedaan (HTTPS) in de tweede op logistiek niveau (op basis van bericht headers WS-addressing/ebMS routingID etc..).

#	Bouwblok	Type	Status	Toelichting
1	Logging, Auditing en Berichtarchivering	DSO	Beschikbaar	Ten behoeve van verantwoording.

Daarnaast maakt het Knooppunt gebruik van herbruikbare bouwblokken die in de GAS Knooppunt Toegang (IAM) zijn beschreven.

6 Netwerk

In dit hoofdstuk wordt de Netwerklaag beschreven van Knooppunt Gegevensuitwisseling, deze is bepalend voor de te kiezen oplossingen.

Op het niveau van de GAS wordt in principe geen uitspraak gedaan over de onderliggende Netwerklaag. Wel worden eisen vanuit het DSO gesteld aan de onderliggende Netwerklaag. De Netwerklaag wordt concreet uitgewerkt in de Overall Project Start Architectuur (OPSA) en de individuele PSA's.

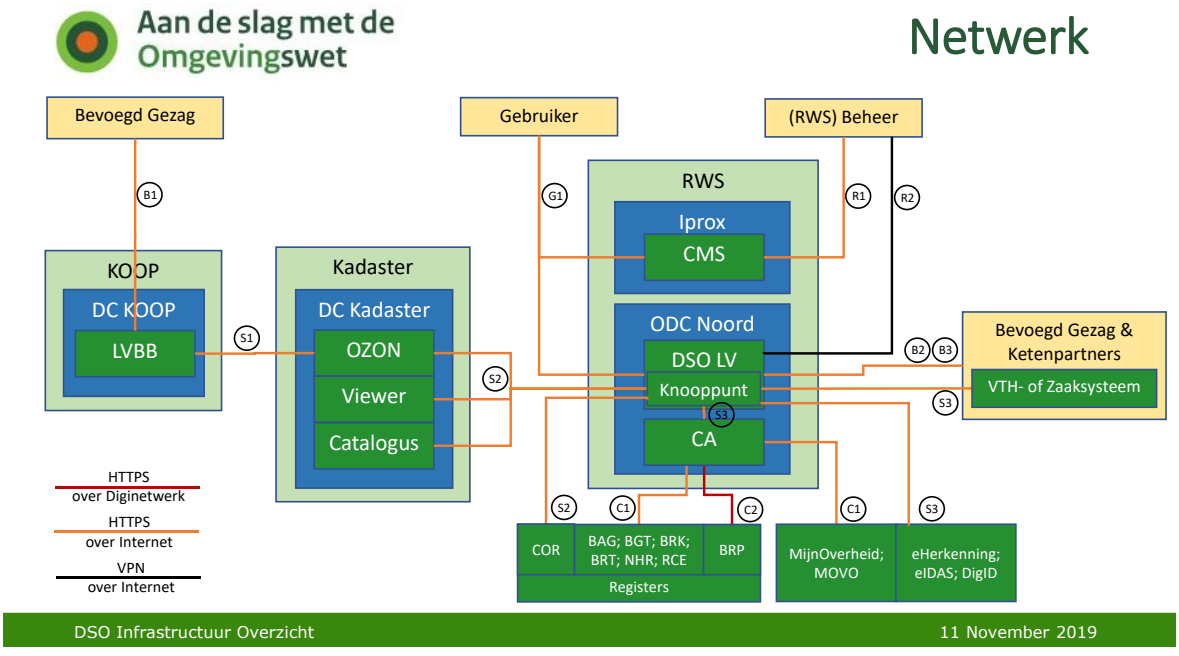
6.1 *Eisen aan Netwerklaag*

In deze paragraaf worden de aanvullingen/uitzonderingen op Netwerklaag beschreven die van toepassing zijn voor deze GAS.

De netwerklaag in de OGAS beschrijft de netwerklaag van het Knooppunt aangezien het Knoopunt het single-point of communication is.

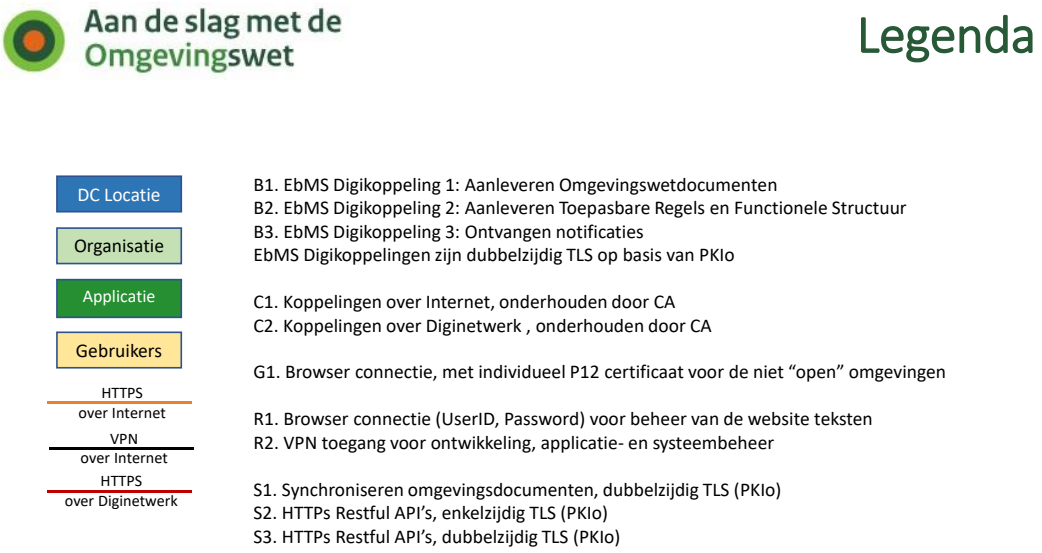
6.2 *Aansluiting andere omgevingen*

In deze paragraaf worden de bouwblokken uit andere omgevingen benoemd waarop een aansluiting noodzakelijk is.



Figuur 14 Netwerklaag

Omgeving	Via	
Kadaster OZON, Viewer, Catalogus	HTTPS/internet	
Centraal Aansluitpunt	HTTPS/internet	
COR, eHerkenning, eIDAS, Digid	HTTPS/internet	
Systemen Bevoegd Gezagen	HTTPS/internet	
Open Stelsel gebruikers	HTTPS/internet	



Figuur 15 legenda Netwerklaag

7 Beheer

In dit hoofdstuk worden de aanvullingen/uitzonderingen op beheeraspecten (benoemd in de OGAS) beschreven die van toepassing zijn voor deze GAS.

Serviceorganisatie

De serviceorganisatie is het aanspreekpunt binnen het DSO voor aansluitproblemen en bij problemen met lopend berichtenverkeer binnen het stelsel. De serviceorganisatie heeft specialistische kennis over standaarden op transport en logistiek niveau en kunnen vragen doorzetten naar service aanbieders daar waar het gaat om problemen met de inhoud van berichten of aansluitproblemen waarvan de oorzaak ligt bij de service aanbieder.

Voor ingewikkelde aansluitproblemen die betrekking hebben op het Knooppunt kunnen zij vragen doorzetten naar de beheer organisatie van het Knooppunt. Deze beschikt over de juiste instrumenten (beheertoepassingen) en kennis om deze aansluitproblemen op te lossen. De serviceorganisatie is dus de eerstelijns helpdesk voor alle problemen rondom berichtuitwisseling en kunnen waar nodig doorzetten naar de tweedelijns ondersteuning (waaronder het beheer van het Knooppunt) binnen het stelsel.

7.1 *Beheertoepassingen*

De volgende beheertoepassingen dienen, aanvullende op de bestaande beheertoepassingen, beschikbaar te zijn:

Binnen het Knooppunt bevindt zich een breed scala aan beheertoepassingen (standaard pakketten en maatwerk) samengevat in onderstaande lijst:

API's (Knooppunt API Store en API Register)
Opvoeren initieel, opvoeren nieuwe versie, wijzigen, verwijderen, publiceren
Gebruik beperken, vrijgeven, blokkeren
Gebruik: rapportages

Verantwoordingsinformatie (auditlog en berichtenarchief)
Auditregels: schonen, verwijderen, inzien
Berichten: schonen, verwijderen, inzien

Autorisaties verbindingen (Knooppunt verschillende componenten)
PKI Certificaten
CPA ebMS
Mandateringen
API-keys

Identiteiten (Knooppunt IS)
Account/Profiel: verwijderen, opschonen
Inlogmiddel: blokkeren

Rol: toekennen, wijzigen
Machtiging: toekennen, blokkeren

In dit hoofdstuk worden de relevante beheer aspecten beschreven als een van de pijlers van een betrouwbare dienstverlening.

7.2 *Serviceniveau*

Al het berichtenverkeer van het DSO loopt via het Knooppunt. In de keten is het Knooppunt een potentiële zwakke schakel die daarom extra aandacht vergt. Wanneer het Knooppunt niet beschikbaar is, geldt dat ook voor het stelsel als geheel. Passende maatregelen zijn nodig om dit te voorkomen. Hierbij past in ieder geval een SLA met de beheerder op basis van 24x7 beschikbaarheid waarin een hoog beschikbaarheids-percentage[6] wordt afgesproken. Voor het kunnen halen van die hoge beschikbaarheid is herstelbaarheid van het grootste belang.

7.3 *Herstelbaarheid*

Een essentieel aspect van beheer is het kunnen herstellen van dingen die fout zijn gegaan. In het hoofdstuk beveiliging wordt nader ingegaan op hoe erg het is als er iets misgaat. Hier worden de instrumenten beschreven die voor herstel gebruikt kunnen worden.

Voor het Knooppunt is het belangrijk om berichten (voornamelijk berichten met juridische consequenties) nogmaals te kunnen verzenden als er iets mis is gegaan. Voor deze her-injectie van berichten wordt het bericht uit het postboek gehaald en opnieuw verstuurd. Hierbij zijn er beperkte mogelijkheden om informatie te herstellen die de oorspronkelijke verzendingsfout veroorzaakte.

Berichten zijn niet het enige wat fout kan gaan. Andere essentiële fouten die hersteld moeten kunnen worden, zijn fouten in de configuratie en uitrol van services. Dit proces is via zelfbediening geautomatiseerd. Door een storing of calamiteit kan de configuratie van het Knooppunt corrupt raken of zelfbediening niet goed functioneren. In die gevallen moet er de mogelijkheid zijn configuraties te herstellen of handmatig op te voeren.

Verschillende services zijn van elkaar te isoleren, waardoor het mogelijk is een service (of set van services) die problemen op het Knooppunt veroorzaakt anders te behandelen. Een berichtenstroom met problemen (abnormaal veel berichten vanwege een aanval of systeemfout) vraagt veel resources en kan het hele Knooppunt in gevaar brengen. Anders behandelen kan dan betekenen volledig afsluiten, maar ook het tijdelijk beperken van de beschikbaarheid van een service zodat het Knooppunt als geheel geen hinder ondervindt van problemen bij één service.

[6] In de PSA zal dit uitgedrukt worden in een meetbare grootheid na verdere analyse van bekende en veronderstelde SLAs. Bijvoorbeeld 99.95%, 99.99% of 99.999%.

7.4 *Beheerprocessen*

Het Knooppunt streeft naar maximale zelfbediening. Dit is gedaan om de beheerlast te beperken en te zorgen dat organisaties zelf eenvoudig, snel en adequaat wijzigingen kunnen doorvoeren in hun eigen gegevens en instellingen. Hierdoor zijn organisaties zelf 'in control' en worden de afhankelijkheden tussen organisaties onderling beperkt. De serviceorganisatie en de beheerders van het Knooppunt kunnen zich daarmee richten op problemen waarvoor specialistische kennis nodig is. Standaardprocessen beheer processen van het Knooppunt worden zoveel mogelijk met zelfbediening geautomatiseerd.

Het proces "Service gebruiken" is de kern van het Knooppunt. In dit proces worden alle berichten van het stelsel uitgewisseld. Daarnaast kent het Knooppunt ondersteunende processen die gebaseerd zijn op de beschrijving van activiteiten die onder service afnemen plaatsvinden. Hierna volgt een beschrijving van de processen.

#	Proces	Toelichting
1	Aanmelden organisatie/persoon	Organisaties en personen moeten eenmalig hun identiteit binnen het stelsel vastleggen om van de zelfbedienings-functionaliteit gebruik te kunnen maken. In de zelfbediening gebruikersinterface wordt dit vastleggen ontsloten, verdere uitwerking rondom identiteiten is te vinden in de GAS Knooppunt Toegang (IAM) [Beveiliging].
2	Ontwikkelen vertaling bericht	In dit proces wordt het ontwikkelen van vertalingen van berichten gerealiseerd. Het gaat bij vertalen om zowel de envelop(translatie) als de inhoud(transformatie). Vertaling van berichten kan onder voorwaarden op het Knooppunt gerealiseerd worden voor stelselonderdelen. Hiervoor moet eerst getoetst worden of de gevraagde vertaling in het Knooppunt thuishoort[7]. De toetsing vindt plaats onder verantwoording van de serviceorganisatie. Indien de toetsing positief is, wordt de vertaling ontwikkeld, getest en uitgerold in combinatie met een service van een aanbieder.
3	Service registreren voor gebruik	Dit bedrijfsproces ondersteunt het registreren van services door aanbieders. Een aanbieder moet alle services van een stelselonderdeel via het Knooppunt aanbieden. De aanbieder geeft per service aan welke functies van het Knooppunt worden gebruikt. Deze informatie wordt vervolgens gebruikt voor het (automatisch) configureren van het Knooppunt en is via service zoeken opvraagbaar.
4	Toegang tot service verlenen	Dit proces ondersteunt het registreren voor gebruik van individuele services. Een afnemer geeft aan welke service(s) hij af wil nemen en het Knooppunt faciliteert dat de afnemer toegang krijgt tot de services(autorisatie is zoveel als mogelijk geautomatiseerd) en dat de aansluiting werkt. In het geval van services met doelbinding zal de aanbieder handmatig toetsen of toegang gegeven wordt aan de afnemer.
5	Service gebruiken	Dit proces ondersteunt het aanroepen van en aanbieden van services. Een afnemer kan alle services via het Knooppunt bevragen. Op basis van de door de aanbieder ingestelde

[7] Een vertaling moet in ieder geval geen business logica bevatten. Filteren van informatie is toegestaan. Aggregeren, orkestreren van services is dat niet.

		functies zet het Knooppunt de vraag door naar de aanbieder en levert het antwoord weer af bij de afnemer.
6	Wijzigen service	Wanneer een service wijzigt (er komt een nieuwere versie) of uit gebruik wordt genomen dan wordt met de afnemers een overgangsperiode afgesproken en krijgt de afnemer tijdig informatie om de afname van de service aan te passen aan de nieuwe situatie. De aanbieder geeft de wijziging vooraf via zelfbediening aan. Vervolgens wijzigt bij ingang van de nieuwe versie na het aflopen van de met de aanbieders afgesproken overgangsperiode (automatisch) de configuratie van het Knooppunt. Het Knooppunt zorgt voor notificaties aan de afnemers (zie [Achtergrond] voor meer informatie).
7	Notificeren afnemer	Wanneer een aanbieder een service wijzigt, moeten afnemers dit weten zodat ze tijdig over kunnen gaan naar een nieuwe versie. Dit proces bepaalt welke afnemers geïnformeerd moeten worden en stuurt hen de voor hen relevante informatie.

#	Proces	Toelichting
8	Service informatie verstrekken	Afnemers die willen aansluiten op het stelsel moeten de juiste service kunnen vinden. Dit proces zorgt ervoor dat informatie over services op het Knooppunt wordt ontsloten. Het gaat hier om technische informatie die voor de aansluiting nodig is. Er wordt ook gezorgd voor verwijzing (via Linked Data) naar de gegevens catalogus voor semantische informatie. Omgekeerd verwijst de stelselcatalogus (met Linked Data) vanuit haar semantische informatie naar de technische informatie over de service op het Knooppunt.
9	Afmelden gebruik	Als een applicatie een service niet meer gebruikt omdat de applicatie wijzigt of uit gebruik wordt genomen dan geeft de afnemer dit aan[8]. Het Knooppunt zorgt automatisch voor notificatie van de aanbieder en wijziging van de configuratie van het Knooppunt.
10	Notificeren aanbieder	Wanneer een afnemer een service niet meer afneemt, wordt de aanbieder met dit proces daarvan op de hoogte gesteld. De aanbieder heeft zo een exact beeld van zijn afnemers en kan een service veilig uit gebruik nemen als alle afnemers zich afgemeld hebben.

#	Proces	Toelichting
11	Ondersteunen gebruik	Dit proces ondersteunt het gebruik. De beheerorganisatie van het Knooppunt krijgt als 2e lijn vragen doorgezet vanuit de serviceorganisatie van het stelsel. Dit zijn vragen die specifiek gaan over het Knooppunt. Ondersteuning van de keten is bij de serviceorganisatie van het stelsel geregeld. Daarnaast wordt gebruik ondersteund door het notificeren van afnemers en aanbieders over wijzigingen.
12	Verstrekken verantwoordingsinformatie	Dit proces ondersteunt het verantwoorden over het verzenden en ontvangen van berichten. Een afnemer of aanbieder die moet verantwoorden welke berichten er gecommuniceerd zijn kan via de serviceorganisatie bij het Knooppunt een verzoek indienen voor informatie over de rol die het knooppunt in de

[8] Geldt niet voor open services die worden anoniem gebruikt een afnemer registreert zich hier niet voor.

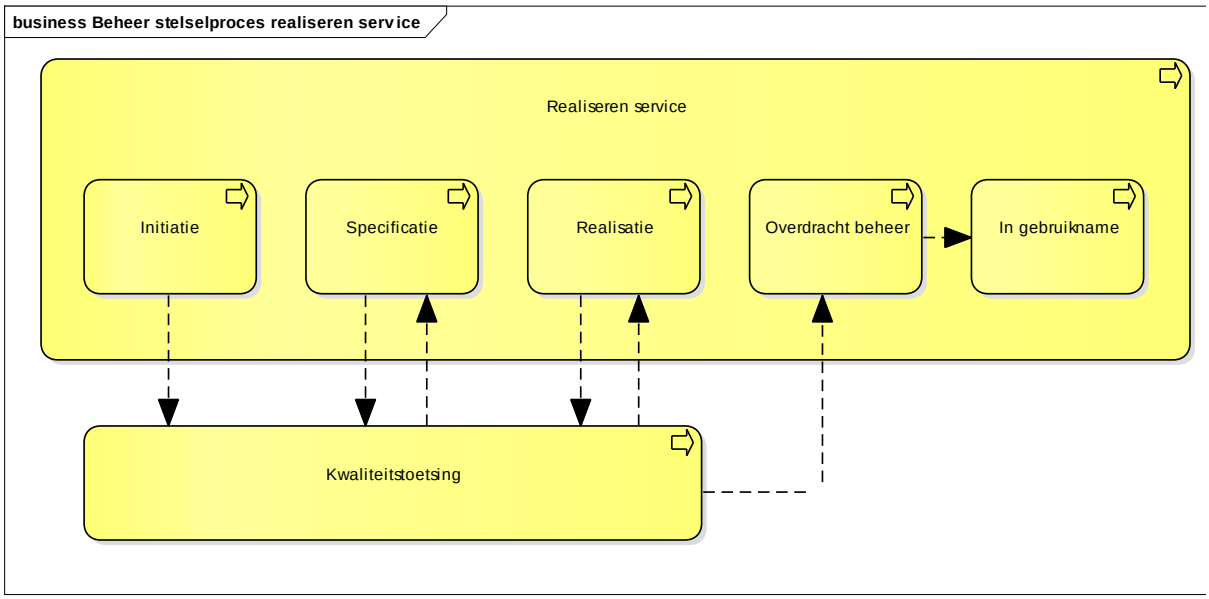
		aflevering heeft gespeeld. Afhandeling wordt beschreven in de GAS beveiliging [Beveiliging] en de GAS serviceorganisatie (beheer inrichten).
13	Service monitoren en rapporteren	Dit proces monitort het gebruik van services en rapporteert hierover. Hierbij worden statistieken verzameld over gebruik en prestaties ten behoeve van rapportages en het signaleren van overschrijden van drempelwaarden die technische problemen met services aanduiden.
14	Servicemanagement	Dit proces voert operationeel en tactisch beheer uit, waar-onder functioneel beheer, technisch beheer, applicatie-ontwikkeling, releasemanagement, productmanagement, etc. De beheerorganisatie bekijkt proactief het verkeer dat door het Knooppunt loopt en neemt maatregelen bij geconstateerde problemen. Problemen kunnen zijn het halen van SLAs, overschrijden van drempelwaarden, cyberaanvallen en het voorkomen van storingen.

7.5 *Processen realiseren services*

Veel primaire functionaliteit van het Knooppunt is al beheer functionaliteit: monitoring, zelfbediening, doelbinding. Hiervoor dienen werkprocessen voor de beheerder van het Knooppunt uitgewerkt te worden. Het proces voor monitoring zal beschrijven welke producten en notificaties geleverd dienen te worden. Het proces rondom doelbinding beschrijft hoe het Knooppunt doelbinding voor zijn afnemers inregelt. Het proces voor zelfbediening is al op hoofdlijnen beschreven in de views van het primaire proces gezien vanuit afnemer en aanbieder. Daarin zijn twee belangrijke aandachtspunten voor beheer:

1. In Figuur 5 is te zien dat autoriseren gebeurt in samenwerking met aanbieders van services. De rol van het Knooppunt is hierin beperkt. Het Knooppunt notificeert de aanbieder van het autorisatieverzoek en biedt de aanbieder de mogelijkheid om het in het portaal goed of af te keuren. Een generieke procesbeschrijving hoe de aanbieder tot een autorisatie beslissing komt ligt buiten scope van het Knooppunt.

2. Het tweede belangrijke aandachtspunt voor beheer is het in gebruik nemen van een service. Het proces van het realiseren van een service ligt in hoofdzaak bij de aanbieder, echter in dit generieke proces zal aandacht moeten zijn voor de kwaliteit van de service. Voordat hij in productie op het Knooppunt aangeboden mag worden zal hij getoetst moeten worden. Als aan de toetsingscriteria is voldaan kan de service in productie worden genomen. Hoe deze toetsing te regelen is een nog open punt.



Figuur 16. Realiseren service in detail

8 Beveiliging en Privacy

In dit hoofdstuk worden de aanvullingen/uitzonderingen op de beveiliging en privacy (benoemd in de OGAS) beschreven die van toepassing zijn voor deze GAS. De relevante beveiliging en privacyaspecten worden beschreven als een pijler voor een betrouwbare serviceverlening. Betrouwbaarheid is in de context van beveiliging en privacy het inbouwen van die mechanismen die bescherming van informatie tot doel hebben.

De aanbieder die de informatie levert, zal moeten inschatten of er risico's spelen bij het aanbieden van informatie via een service. De aanbieder moet de baseline informatiebeveiliging overheid (BIO) toepassen. Deze is vereist voor het hele stelsel. Uitgangspunt is dat informatie binnen het stelsel hooguit departementaal vertrouwelijk is. Het Knooppunt moet een passend beveiligingsniveau kunnen bieden bij de uitkomst van deze risicoanalyse door de aanbieder.

8.1 *BIV-classificaties*

In de volgende tabel wordt voor resources en de betrokken capabilities de classificatie geduid op basis van de classificering zoals beschreven in de OGAS.

8.1.1 *Beschikbaarheid*

Resource		
	Classificatie	Toelichting
Beschikbaar stellen Knooppunt	Hoog	Bij uitval staan de meeste ketens binnen DSO helemaal stil. Een single point of communication is ook een singe point of failure.

8.1.2 *Integriteit*

Resource		
	Classificatie	Toelichting
Beschikbaar stellen Knooppunt	Hoog	De betrouwbaarheid van de doorgifte van informatie waarop afnemers vertrouwen moet boven iedere twijfel verheven staan en kan juridische gevolgen hebben.

8.1.3 *Vertrouwelijkheid*

Resource		
	Classificatie	Toelichting

Beschikbaar stellen Knooppunt	Midden	Er gaan veel stromen over het Knooppunt doch er zullen maar een beperkt aantal zijn waarvoor vertrouwelijkheid echt cruciaal is.

Onderstaand worden de classificaties nader toegelicht.

8.1.4 *Beschikbaarheid*

Het Knooppunt vervult een centrale rol in het DSO, uitval van het Knooppunt is zeer onwenselijk, er dienen dus maatregelen genomen te worden die de beschikbaarheid van het Knooppunt (zoveel mogelijk) garanderen. Dit zijn maatregelen op een aantal vlakken: capaciteit, calamiteit en bescherming tegen aanvallen.

Capaciteit
Voor het garanderen van de beschikbaarheid moet het Knooppunt de capaciteit hebben om de vraag vanuit het DSO aan te kunnen. Het gaat hierbij om capaciteit op netwerkgebied (bandbreedte) en server capaciteit (verwerking). Er worden maatregelen genomen om deze te kunnen garanderen. Eén van deze maatregelen is het werken met een geclusterde omgeving welke de vraag over meerdere servers verdeelt. Een zogenaamde "active-active" verdeling, meerdere instanties kunnen tegelijkertijd samenwerking als één geheel.

Calamiteit
Er zijn allerlei soorten calamiteiten mogelijk die de uitval van het Knooppunt tot gevolg kunnen hebben. Van een natuurramp tot een graafmachine die een netwerk-kabel doorsnijdt tot een menselijk fout waardoor de software vastloopt. Er worden maatregelen genomen om de kans dat een calamiteit leidt tot uitval te minimaliseren. De "active-active" verdeling is een van deze maatregelen, die zorgt ervoor dat het mogelijk is om met meerdere locaties te werken zodat bij een calamiteit op een locatie de andere blijft werken.

Bescherming tegen aanvallen
Er worden maatregelen genomen tegen hacks en DDOS aanvallen, dit kan gedeeltelijk via services die de netwerk- en hostingproviders bieden en gedeeltelijk in de configuratie van de Toegangspoort in het Knooppunt door maatregelen te nemen die het aantal requests per seconde voor één gebruiker maximeren (throtteling). Voor de goede werking hiervan moeten gebruikers zich altijd authenticeren voor het gebruik van een service met gegarandeerde beschikbaarheid.

De beschikbaarheid van het product Knooppunt moet worden geclassificeerd als hoog[9]. Als de beschikbaarheid het laat afweten, zal dit weliswaar voor de meeste capabilities slechts leiden tot vragen en klachten van de gebruikers en vragen aan het management. Wanneer echter "Afnemen service" niet beschikbaar is staat het hele stelsel stil wat zal snel leidt tot verdere escalaties. Zie Bijlage C: Beveiligingsclassificaties voor een detaillering per capabilities.

[9] Zie bijlage C voor definitie.

8.1.5 *Integriteit*

Veel van de informatie die over het Knooppunt loopt is open, echter de integriteit van die informatie is belangrijk. Doordat al het berichtenverkeer met het Knooppunt versleuteld is kan gegarandeerd worden dat de informatie tijdens transport niet aangepast is en tevens van de authentieke bron afkomstig is. Informatie geleverd door het Knooppunt is daarmee betrouwbaar.

In het Knooppunt wordt zonering toegepast. Daarmee hoeven alleen die gedeeltes die met gesloten informatie te maken hebben onder een zwaarder regime te vallen.

Het Knooppunt biedt via "Service afnemen" een groot deel van haar services aan derden aan via internet. De services op het Knooppunt zullen moeten voldoen aan de beveiligingsrichtlijnen van het NCSC [NCSC webrichtlijnen]. Aan de hand hiervan worden maatregelen genomen die voorkomen dat kwaadwillende de integriteit van het Knooppunt kunnen aantasten.

De integriteit van het product Knooppunt moet worden geclassificeerd als hoog[10]. Als de integriteit het laat afweten zal dit serieuze juridische gevolgen kunnen hebben. Zie Bijlage C: Beveiligingsclassificaties voor een detaillering per capabilities.

8.1.6 *Vertrouwelijk*

Het Knooppunt ontsluit services die naar verwacht volume vooral open data zullen aanbieden. Toch wordt al het berichtenverkeer versleuteld[11] en wordt voor alle services met garanties over beschikbaarheid een vorm van authenticatie vereist. De versleuteling is er om de privacy van de gebruiker te waarborgen, de informatie is wel open, maar wat de individuele gebruiker opvraagt is dat niet. De versleuteling waarborgt de privacy, de authenticatie is voor waarborgen van de privacy bij open data niet noodzakelijk maar de authenticatie wordt toch ingezet om de beschikbaarheid beter te kunnen garanderen. Er is echter ook een minderheid aan services die wel vertrouwelijke informatie bevat. Hiervoor dient de authenticatie, autorisatie en versleuteling dus wel om vertrouwelijkheid van de informatie zelf te garanderen. Het gaat hierbij op zijn hoogst om departementaal vertrouwelijke informatie. Er zijn hogere kwalificaties binnen de overheid.

De vertrouwelijkheid van het Knooppunt wordt geclassificeerd als midden[12]. Als de vertrouwelijkheid het laat afweten zal dit, maar voor een beperkt aantal berichtstromen, gevolgen hebben.

Naast de beveiligingsclassificatie gaat dit hoofdstuk ook iets dieper in op authenticatiemiddelen, Authenticatie & Autorisatie en onweerlegbaarheid.

---

[10] Zie bijlage C voor definitie.

[11] Met versleuteling wordt de transportlaag bedoeld, niet de berichtinhoud. HTTP transport wordt minimaal met enkelzijdig TLS versleuteld, de afnemer hoeft zich dan niet te authenticeren. De afnemer weet daarmee zeker dat hij de authentieke bron aanspreekt en dat zijn vragen niet afgeluisterd worden.

[12] Zie bijlage C voor definitie en verdere toelichting

8.2 *Authenticatiemiddelen*

Beveiliging is een belangrijk aspect dit kent een eigen GAS. Met het oog op beheer en consistentie wordt dit op één plek en éénmalig gedefinieerd. Beveiliging mag niet afhankelijk zijn van de discipline van ontwikkelaars. Applicaties en beveiliging zijn daarom ontkoppeld.

Voor het verkrijgen van toegang tot beveiligde informatie is authenticatie en autorisatie van de eindgebruiker nodig. Authenticatiemiddelen kunnen persoonsgebonden zijn (burger, medewerker van een bedrijf of ambtenaar) of organisatie gebonden (eigenaar stelselvoorziening, bevoegd gezag). Authenticatiemiddelen en hun eigenschappen worden verder uitgewerkt in de GAS Knooppunt Toegang (IAM). Het Knooppunt maakt hergebruik van de functionaliteiten die Beveiliging biedt.

8.3 *Authenticatie en Autorisatie*

De Toegang controle component wordt door het Knooppunt gebruikt voor het authenticeren en autoriseren van systemen. De Toegang controle component is ook zelfstandig te gebruiken door stelselvoorzieningen. Front-end toepassingen, zoals de API Manager van het Knooppunt en Omgevingsloket, maken gebruik van de Toegang personen component om gebruikers toegang te verlenen. Voor beide componenten wordt in ieder geval gebruik gemaakt van Role Based Acces Control (RBAC). De Toegang controle en Toegang personen componenten zullen ontwikkeld worden door het project Beveiliging (PR29) en staan in bijbehorend GAS uitgebreid beschreven.

Systemen overheden
Systemen gebruiken bij het aanroepen van beveiligde services PKIoverheid of OAuth om zich te authenticeren. Organisaties (bedrijven en overheden) die PKIoverheid gebruiken koppelen het publieke deel van hun PKIoverheid certificaat via zelfbediening aan hun voor het stelsel vastgelegde identiteitsgegevens. In het geval van PKIoverheid certificaat autoriseert het Knooppunt altijd op organisatieniveau. OAuth wordt ook via zelfbediening geconfigureerd, de Toegang controle component verzorgt de OAuth tokens.

Applicaties en apps derden
In het geval van applicaties en apps van derden biedt de Toegang controle component OAuth aan. Applicaties en apps van derden mogen zelf geen DigiD of eHerkenning implementeren. OAuth biedt mogelijkheden waarmee gebruikers van deze apps geautoriseerd kunnen worden zonder dat deze apps DigiD of eHerkenning hoeven te implementeren. DigiD en eHerkenning worden in combinatie met OAuth ingezet waarbij applicaties en apps van derden geen toegang tot inloggegevens of ID’s van DigiD of e-Herkenning hebben. De volledig beschrijving van deze oplossing volgt in de PSA.

Identity propagation
De vorige paragraaf gaf al aan dat de identiteit van de afnemer doorgegeven kan worden (identity propagation) aan de achterliggende service die door het Knooppunt wordt ontsloten. Dit is noodzakelijk omdat er gevallen zijn waarbij een fijnmazige autorisatie noodzakelijk is op functie- of dataniveau. Dit kan alleen in de service zelf

plaatsvinden. Business logica is dan nodig om de autorisatie binnen een service te regelen.
Bijvoorbeeld: bij beheerservices van de Catalogus kan het Knooppunt alleen grofmazige toegang tot de hele service verlenen. Welke informatie de service bewerkt kan worden (fijnmazige autorisatie) wordt bepaald door de service zelf op basis van doorgegeven identiteitsinformatie (inclusief rol) en de eigen business logica (welke gegevens van welke bronhouder zijn). Het Knooppunt en de Toegang controle component ondersteunen dus geen Attribute Based Acces Control (ABAC). Het is aan service aanbieders zelf om dit in te regelen.
Voor het doorgeven van identiteit zijn er internationale interoperabiliteitsstandaarden. Voor REST gebaseerde services is OAuth[13] de "de facto" interoperabiliteitsstandaard. Voor SOAP/WSDL is dat SAML.

8.4 *Onweerlegbaarheid*

Het Knooppunt ontsluit services die gebruikt worden in processen die juridische gevolgen hebben, denk bijvoorbeeld aan vergunningaanvragen, waar het Knooppunt een aanvraag ingediend in het webportaal doorzet naar het bevoegd gezag. Op een later tijdstip moet er verantwoording kunnen worden afgelegd: wanneer een aanvraag verzonden is, wanneer hij is afgeleverd bij bevoegd gezag en het bericht zelf. In dit voorbeeld gaan op basis hiervan wettelijke termijnen lopen. Het is mogelijk om berichten via het Knooppunt onweerlegbaar te versturen. Dat wil zeggen dat later aangetoond kan worden dat een bericht op een bepaald moment intact is ontvangen of verstuurd. Dit vraagt ook om een hoge mate van integriteit anders kan de claim van onweerlegbaarheid niet waargemaakt worden.

Meerdere niveaus van onweerlegbaarheid kunnen, afhankelijk van de eisen die het proces stelt, worden toegepast:

- Laag - Alleen audit informatie bijhouden
- Midden - Audit informatie en berichtarchief bijhouden
- Hoog - Audit informatie, berichtarchief bijhouden en de berichten worden getekend.

De auditing component en berichtarchivering nemen maatregelen die ervoor zorgen dat wat eenmaal in deze componenten is vastgelegd niet gemanipuleerd kan worden. Bij laag en midden wordt het Knooppunt vertrouwd: het gaat correct en integer om met berichten. Wanneer het proces dermate gevoelige informatie bevat dat vertrouwen in het Knooppunt niet te rechtvaardigen is kan het tekenen van berichten zelf worden toegepast. Dit is een zwaar middel voor afnemers en aanbieders van services en moet daarom alleen toegepast worden als het echt noodzakelijk is.

[13] OAuth is op dit moment geen e-overheid standaard maar wel voorgedragen voor opname op de "pas toe of leg uit" lijst van het forum standaardisatie.

9 Transitie

In dit hoofdstuk worden de specifieke onderwerpen van de transitie beschreven die van toepassing zijn voor deze GAS.

De scopefasering Knopppunt die hieronder kort is samengevat is de leidraad voor de architectuurtransitie van het Knooppunt gegevensuitwisseling

9.1 *Scopefasering Knooppunt gegevensuitwisseling*

Tijdens de realisatie van het Knooppunt is gebleken dat het architectuureinddoel niet binnen de gewenste termijn kan worden afgerond. Dit mede door de afhankelijkheid van het CA (Centraal Aansluitpunt) en de onzekerheid over de schaalbaarheid van de standaard componenten (WSO2). De oplossing is gezocht in het aanpassen van de scope van het Knooppunt voor 2020 (tot vlak vóór inwerkingtreding Omgevingswet) en te sturen op een minimum viable product waarvan de meerwaarde van ieder onderdeel praktisch helder is.

Vervolgens kan tussen 2020 en 2024 gewerkt worden aan de uiteindelijke realisatie van alle functionaliteit van het Knooppunt zoals beoogd in de GAS en PSA van het Knooppunt, danwel nieuwe prioriteiten worden gesteld op basis van nieuwe voortschrijdende inzichten.

9.2 *Analyse*

Voor de analyse van het minimum viable product wordt gekeken langs de assen:

- DSO specifiek en niet DSO specifiek
- Muteren (incl. aanleveren) en Bevragen

9.2.1 *Niet DSO specifieke services niet via het Knooppunt*

Services/APIs die niet specifiek voor het DSO zijn ontwikkeld en dus al een bestaand bekend endpoint hebben bij de aanbieder van deze service/API (Denk bijvoorbeeld aan de BRT achtergrondkaart, basisregistraties.) worden niet via het Knooppunt gerouteerd. Deze services/APIs zijn wel in de zelfbedieningswinkel (API store) terug te vinden. Dit scheelt aanzienlijk in het volume van berichtenverkeer dat over het Knooppunt moet lopen (zie ook OGAS ondersteunende capabilities – beschikbaar stellen omgevingen).

Niet DSO specifieke services voor aanleveren/muteren die nu al niet via het knooppunt lopen blijven ook buiten het knooppunt (voorbeelden zijn het aanleveren van omgevingsdocumenten door bevoegd gezag aan de LVBB en het aanleveren van gegevens door bronhouders aan Leveranciers van Omgevingsinformatie).

9.2.2 *DSO specifieke services via Knooppunt wordt een keuze*

DSO specifiek Aanleveren/muteren altijd via Knooppunt
Dit zijn services waarmee informatie wordt aangeleverd aan het DSO of waarmee het DSO informatie aflevert aan BG. Het gaat hier om transacties waarbij het aanleveren van informatie een verandering in de informatie huishouding tot gevolg kan hebben. Denk hierbij aan het aanleveren van toepasbare regels door Bevoegd gezag aan het DSO of het doorgeven van meldingen en aanvragen van het DSO naar bevoegd gezag.

Deze services maken vrijwel allemaal gebruik van transformatie & translatie als ook berichtarchivering en auditing en mogelijk ook onweerlegbaarheid, signing en encryptie functionaliteit. Het knooppunt biedt hier echt meerwaarde, tegelijkertijd zit er naar verwachting weinig volume in deze berichtenstroom zodat het Knooppunt geen (grote) aanpassingen op performance gebied nodig heeft om deze te verwerken.

DSO specifiek bevragen
Dit zijn services waarmee informatie alleen kan worden opgehaald en die specifiek voor het DSO ontwikkeld zijn. Denk hierbij vooral aan de informatie producten van informatiehuizen. Voor deze services geldt dat ze vrijwel altijd gebruik maken van routeren en authenticatie en autorisatie. Het Knooppunt biedt hier lang niet altijd meerwaarde.

Op dit moment is meerwaarde alleen zeker voor services die aangeboden worden vanuit OBO-RWS componenten en OZON of wanneer ook gebruik gemaakt wordt van aanvullende functionaliteit zoals auditing, berichtarchivering, transformatie & translatie. Dit laatste zal echter bij een kleine minderheid van de services het geval zijn. Per service/API zal op basis van een nader te definiëren procedure een keuze worden gemaakt of deze via het Knooppunt gerouteerd wordt of dat deze rechtstreeks benaderbaar is.

9.3 ***Zelfbediening***

Een service/API wordt in alle gevallen geadverteerd in de API store van het Knooppunt, of het berichtenverkeer nu over het knooppunt loopt of niet. Dit levert voor afnemers één centrale ingang op tot het DSO. Ze kunnen alle informatie om services/APIs binnen het DSO te gebruiken op één plek vinden. Van hieruit kunnen via OAS3 de services ook worden gepubliceerd op het ontwikkelaarsportaal.

Zelfbediening voor aanbieders was met name voorzien om beheer te minimaliseren wanneer alle services via het Knooppunt liepen. Indien door bovenstaande maatregelen het aantal service op het Knooppunt terug loopt kan afgezien worden van verdere ontwikkeling.

Zelfbediening voor afnemers biedt duidelijk meerwaarde met het overzicht van alle services die geboden wordt. De primaire focus van zelfbediening wordt het bieden van dit overzicht en niet de integratie met de rest van de Knooppunt functionaliteit. Dit kan (i.s.m. Kadaster) stapsgewijs uitgebreid worden met meer functionaliteit voor dit overzicht en differentiatie naar servicelevels.

9.4 *Samenvatting*

In een was/wordt overzicht (huidige/beoogd) wordt de voorgestelde scopeaanpassing samengevat:

- Fysiek berichtenverkeer: **huidige** scope al het verkeer binnen DSO loopt via het Knooppunt (DSO specifieke en niet DSO specifieke services voor bevragen, aanleveren en muteren), **beoogde** scope alleen verkeer op basis van meerwaarde loopt via het Knooppunt.
- Zelfbediening service aanbod: geen scopeaanpassing (één winkel met alle APIs).
- Zelfbediening afnemers: **huidige scope** volledige zelfbediening, **beoogde** scope focus op informatie voor afnemen, geen integratie met andere Knooppunt functionaliteit.
- Zelfbediening aanbieders: **huidige** scope volledige zelfbediening, **beoogde** scope géén zelfbediening, realisatie door inrichten beheer proces.
- Authenticatie: **huidige** scope voor alle DSO projecten, **beoogde** scope voor OBO-RWS componenten en OZON.
- Autorisatie: **huidige** scope voor alle DSO projecten, **beoogde** scope voor OBO-RWS componenten en OZON.
- Auditing, berichtarchivering: **huidige** scope voor alle services/APIs, **beoogde** scope voor alle services/APIs met juridische gevolgen.
- Onweerlegbaarheid Signing & Encryptie: **huidige** scope beschikbaar voor alle services/APIs, **beoogde** scope voor sommige services/APIs met juridische gevolgen.
- Transformatie & Translatie: **huidige** scope voor alle DSO projecten, **beoogde** scope voor OBO-RWS componenten en OZON.
- Doelbinding: **huidige** scope voor alle DSO projecten, **beoogde** scope voor OBO-RWS componenten en OZON.

Bijlage A: Bronnen

In deze bijlage worden de voor dit document gebruikte bronnen beschreven.

Interne bronnen:

Referentie	Document	Omschrijving
1	GAS Knooppunt	1.6
2	DSO – Voorstel aanpassing scope Knooppunt 2019	v2
3	DSO – Impact analyse scope fasering Knooppunt	1.01
4	Nadere invulling ontwikkelaarsportaal en API store	1.0
5	DSO Organisatie	1.0

Overige en externe bronnen:

Referentie	Document	Omschrijving
[OGAS]	Binkhorst, V. (2017). Overall Globale Architectuur Schets. 1.5. Den Haag: Programma Digitaal Stelsel Omgevingswet.	Dit is de overkoepelende kapstok met algemene kaders en richtlijnen voor het stelsel waar de GAS'en van de individuele projecten aan moeten voldoen. In de OGAS wordt de werking van het stelsel en de belangrijkste functies beschreven. Het geeft aan wat de plek van functies en actoren zijn in het stelsel, wat hun onderlinge relaties zijn en wat de afbakening van het stelsel is. Het OGAS bevat ook een API en URI strategie alsmede de lijst met bouwblokken.
[Beveiliging]	Stoelinga, M. (2017) GAS IAM. 0.53 Den Haag: Programma Digitaal Stelsel Omgevingswet.	De GAS van PR29: Beveiliging IAM
[Architectuurschets]	Van Weel, A. (2013). Architectuurschets van het stelsel voor gegevensuitwisseling. 1.0. Den Haag: Logius.	De architectuurschets van het stelsel voor gegevensuitwisseling is opgesteld in het kader van Digikoppeling 3.0 http://wiki.stelselvanoverheidsgegevens.nl/index.php/Architectuurschets
[NCSC Richtlijnen]	Beveiligingsrichtlijnen voor webapplicaties. September 2015. Den Haag: NCSC	De ICT-Beveiligingsrichtlijnen voor Webapplicaties van het Nationaal Cyber Security Centrum (NCSC) vormen een leidraad voor het veiliger ontwikkelen, beheren en aanbieden van webapplicaties en bijbehorende infrastructuur. https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-webapplicaties.html
[Achtergrond]	Terpstra, F. (2016). Achtergrondinformatie Knooppunt. 0.5 Den Haag: RWS	Document met achtergrondinformatie over het Knooppunt. Te vinden op sharepoint ->architectenbureau->documenten->GAS->Knooppunt .
[Standaarden]	Terpstra, F. (2016). Standaarden GAS Knooppunt. 1.35 Den Haag: RWS	Document waarin de standaarden van het Knooppunt benoemd worden. Te vinden op sharepoint ->architectenbureau->documenten->GAS->Knooppunt .

Bijlage C: Beveiligingsclassificaties

Deze bijlage bevat de beveiligingsclassificaties voor het Knooppunt. In het Overall GAS [OGAS] is inmiddels een nieuwere versie van de beveiligingsclassificaties beschikbaar. Verdere uitwerking daarvan gebeurd indien nodig in de PSA.

Classificatie	Toelichting
Beschikbaarheid	Hoe vaak en wanneer een component toegankelijk is en kan worden gebruikt.
Integriteit	Het in overeenstemming zijn van informatie met het afgebeelde deel van de werkelijkheid en dat niets ten onrechte is achtergehouden of verdwenen (juistheid, volledigheid en tijdigheid). Het gaat hier om de integriteit van gegevens waarop en waarmee een component werkt.
Vertrouwelijkheid	Het beperken van de bevoegdheden en de mogelijkheden tot muteren, kopiëren, toevoegen, vernietigen of kennisnemen van informatie tot een gedefinieerde groep van gerechtigden.
Onweerlegbaarheid	Het kunnen aantonen dat informatie door de verzender is geleverd op een manier die juridisch stand houdt.

Waarde	Niet voldoen leidt tot
Zeer Hoog	Maatschappelijke onrust; levensbedreigende situaties; grote financiële gevolgen voor de Nederlandse overheid.
Hoog	Financiële consequenties (op den duur); vragen/klachten bij het management; vragen in de Raad van Toezicht of door de Minister; negatieve publiciteit.
Midden	Vragen/klachten bij gebruikers/klanten; vragen/klachten bij het management.
Laag	Geen gevolgen (alleen vervelend).
Zeer Laag	Niet relevant/niet van toepassing.

In de volgende tabel wordt per capabilities de classificatie voor beschikbaar geduid.

Capabilities	Classificatie	Toelichting
Identiteit aanmelden	Midden	Het niet werken van deze service zal op zijn hoogst leiden tot klachten van gebruikers en vragen aan het management.
Vertalen bericht	Laag	Een continue beschikbaarheid is niet van toepassing bij het ontwikkelen van vertalingen
Zoeken services	Midden	Het niet werken van deze service zal op zijn hoogst leiden tot klachten van gebruikers en vragen aan het management.
Service aanmelden	Midden	Het niet werken van deze service zal op zijn hoogst leiden tot klachten van gebruikers en vragen aan het management.
Service registreren voor afname	Midden	Het niet werken van deze service zal op zijn hoogst leiden tot klachten van gebruikers en vragen aan het management.
Notificeren	Midden	Het niet werken van deze service zal op zijn hoogst leiden tot klachten van gebruikers en vragen aan het management.

Afnemen service	Hoog	Vanwege de grote groep afhankelijke gebruikers (het hele stelsel ligt plat) zal dit snel tot serieuze escalaties leiden.
Aanbieden service	Hoog	Vanwege de grote groep afhankelijke gebruikers (het hele stelsel ligt plat) zal dit snel tot serieuze escalaties leiden.
Ondersteunen gebruik	Midden	Het niet werken van deze service zal op zijn hoogst leiden tot klachten van gebruikers en vragen aan het management.
Servicemanage-ment	Midden	Het niet werken van deze service zal op zijn hoogst leiden tot klachten van gebruikers en vragen aan het management.
Monitoren gebruik	Midden	Het niet werken van deze service zal op zijn hoogst leiden tot klachten van gebruikers en vragen aan het management.
Verantwoorden berichtenverkeer	Hoog	Het niet werken van deze service zal op zijn hoogst leiden tot klachten van gebruikers en vragen aan het management.

In de volgende tabel wordt per capabilities de classificatie geduid voor integriteit geduid.

Capabilities	Classificatie	Toelichting
Identiteit aanmelden	Midden	Het incorrect werken van deze service zal op zijn hoogst leiden tot klachten van gebruikers en vragen aan het management.
Vertalen bericht	Midden	Het incorrect werken van deze service zal op zijn hoogst leiden tot klachten van gebruikers en vragen aan het management.
Zoeken services	Midden	Het incorrect werken van deze service zal op zijn hoogst leiden tot klachten van gebruikers en vragen aan het management.
Service aanmelden	Midden	Het incorrect werken van deze service zal op zijn hoogst leiden tot klachten van gebruikers en vragen aan het management.
Service registreren voor afname	Midden	Het incorrect werken van deze service zal op zijn hoogst leiden tot klachten van gebruikers en vragen aan het management.
Notificeren	Midden	Het incorrect werken van deze service zal op zijn hoogst leiden tot klachten van gebruikers en vragen aan het management.
Afnemen service	Hoog	De betrouwbaarheid van informatie is heel belangrijk in het stelsel bijna alle informatie van het stelsel loopt via het Knooppunt, integriteit is bij het afnemen van service dus zeer belangrijk. Bovendien heeft het gebruik van een aantal services juridische gevolgen.
Aanbieden service	Hoog	De betrouwbaarheid van informatie is heel belangrijk in het stelsel bijna alle informatie van het stelsel loopt via het Knooppunt, integriteit is bij het aanbieden van service dus zeer belangrijk. Bovendien heeft het gebruik van een aantal services juridische gevolgen.
Ondersteunen gebruik	Midden	Het incorrect werken van deze service zal op zijn hoogst leiden tot klachten van gebruikers en vragen aan het management.

Servicemanage-ment	Midden	Het incorrect werken van deze service zal op zijn hoogst leiden tot klachten van gebruikers en vragen aan het management.
Monitoren gebruik	Midden	Het incorrect werken van deze service zal op zijn hoogst leiden tot klachten van gebruikers en vragen aan het management.
Verantwoorden berichtenverkeer	Hoog	Deze service heeft juridische gevolgen, het niet kloppen van geleverde informatie, kan leiden tot negatieve publiciteit of vragen aan de minister.

In de volgende tabel wordt per capabilities de classificatie voor vertrouwelijkheid geduid.

Capabilities	Classificatie	Toelichting
Identiteit aanmelden	Midden	Identiteitsinformatie is van de gebruiker en dus geen open data. Kenmerken van overheden en bedrijven zijn openbare informatie, die van burgers kan wel gevoelig zijn.
Vertalen bericht	Laag	Bericht vertalingen bevatten geen vertrouwelijke informatie het zijn regels voor uitvoeren van vertalingen. Zelfs al bevat de te vertalen informatie vertrouwelijke gegevens de vertalingsregels zelf zijn dit niet.
Zoeken services	Laag	Beschrijvende informatie van services voor het overgrote deel publiek. De beschrijving van sommige services met toegangsbeperking en die met doelbinding is dat misschien niet maar bevat geen gevoelige informatie.
Service aanmelden	Midden	Het aanbieden van een service mag alleen gebeuren door de eigenaar van een service. Deze capabilities mag dan ook alleen voor hen toegankelijke zijn.
Service registreren voor afname	Midden	Het registreren voor afname van een service mag alleen door de afnemer zelf gebeuren. Deze capabilities mag dan ook alleen voor hen toegankelijke zijn.
Notificeren	Laag	Hoewel notificaties geen gevoelige informatie bevatten zijn ze alleen voor de ontvanger bedoeld.
Afnemen service	Midden	Veel services in het stelsel bevatten open data. Een aantal kunnen echter departementaal vertrouwelijke informatie bevatten.
Aanbieden service	Midden	Veel services in het stelsel bevatten open data. Een aantal kunnen echter departementaal vertrouwelijke informatie bevatten.
Ondersteunen gebruik	Midden	Het incorrect werken van deze service zal op zijn hoogst leiden tot klachten van gebruikers en vragen aan het management.
Servicemanage-ment	Midden	Het incorrect werken van deze service zal op zijn hoogst leiden tot klachten van gebruikers en vragen aan het management.
Monitoren gebruik	Laag	De uitkomst van deze service is niet noodzakelijk voor iedereen bedoeld maar bevat geen gevoelige informatie

Verantwoorden berichtenverkeer	Hoog	De verantwoordingsinformatie kan tot departementaal vertrouwelijke informatie uit berichtenverkeer bevatten.