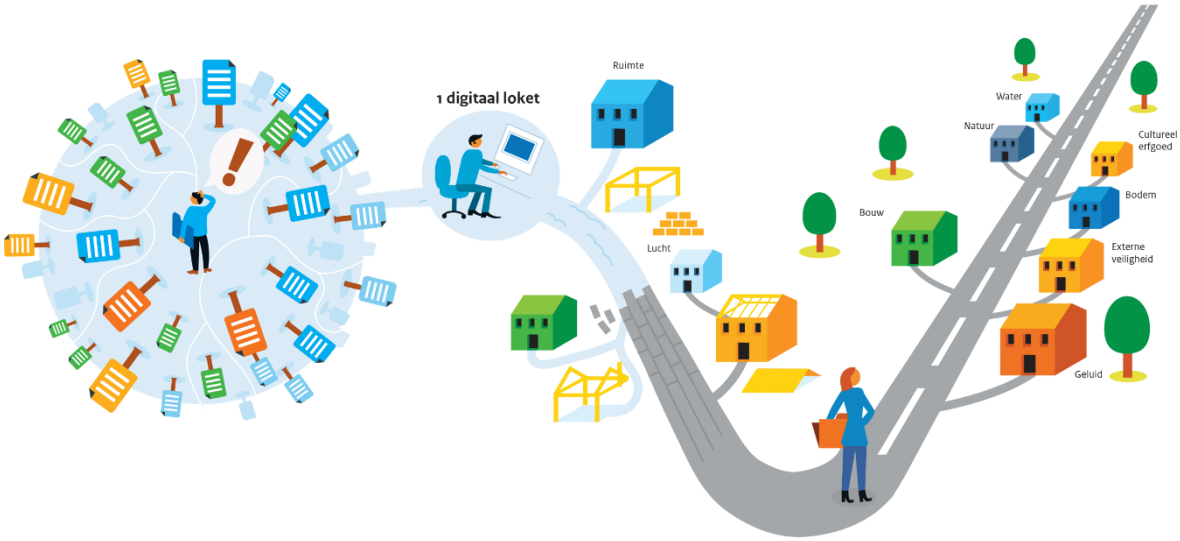
Programma
Aan de slag met de
Omgevingswet

Deelprogramma
Digitaal Stelsel Omgevingswet

Globale Architectuur Schets
Knooppunt Toegang (IAM)

Versie 2.0 Definitief 9 januari 2020



Colofon

Titel	:	Globale Architectuur Schets Knooppunt Toegang (IAM)
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
0.53	Definitief	06-05-2016	M. Stoelinga B. Crompvoets	Bronversie
1.90	Concept	25-10-219	B. Crompvoets	Nieuwe opzet GAS en actualisatie.
1.91	Concept	06-11-2019	B. Crompvoets	Diagram Informatieuitwisseling alsnog van pijlen voorzien.
1.92	Concept	21-11-2019	B. Crompvoets	Reviewcommentaar provincies en gemeentes verwerkt.
2.0	Definitief	09-01-2020	B. Crompvoets	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 Toegang (IAM)

> De primaire verantwoordelijkheid die aan het componentcluster Knooppunt Toegang (IAM) is toegekend is de identificatie, authenticatie, (roltoekenning voor) autorisatie en machtigen van natuurlijke personen.

In een dienstgerichte architectuur vertaalt zich dit in de ondersteuning van de werking van DSO-LV middels Toegangsservices voor inloggen van zowel burgers, medewerkers van bedrijven als medewerkers van het bevoegd gezag. Dit zowel binnenlands, europees als buitenlands. Toegang geschiedt zowel via het eigen Omgevingsloket als het Open Stelsel middels toegangsservices. Daarnaast is ook voorzien dat personen en organisaties anderen kunnen machtigen om namens hen handelingen te verrichten ook met rechtsgevolgen.

Er wordt zoveel mogelijk gebruik gemaakt van GDI services om de toegangsservices te realiseren, met name voor registratie van identiteiten en machtigingsverlening en uitvoeren van authenticatie en machtigingsgebruik. De implementatie van Toegang geschiedt grotendeels middels Identity Access Management voorzieningen zodat Toegang en IAM als termen vaak door elkaar heen worden gebruikt.

N.B. Toegang van services, apps en systeem-systeem verbindingen wordt behandeld in de GAS Knooppunt Gegevensuitwisseling.

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 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 wordt de Grondslagen-laag beschreven, en de aanvullingen/uitzonderingen op de principes (benoemd in de OGAS)

In hoofdstuk 3 wordt de Organisatielaag beschreven.

In hoofdstuk 4 wordt de Informatielaag beschreven en de aanvullingen/uitzonderingen op de standaarden (benoemd in de OGAS) die van toepassing zijn voor deze GAS.

In hoofdstuk 5 wordt de Applicatielaag beschreven.

In hoofdstuk 6 wordt de Netwerklaag 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.

Bijlage B betreft een lijst met begrippen

2 Grondslagen

In dit hoofdstuk wordt ingegaan op de kaders die van toepassing zijn op de positie en rol van Knooppunt Toegang (IAM), 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:

Bijlage B van de doelarchitectuur bevat een opsomming van de voor DSO relevante wetten. Daarvan zijn voor Toegang (IAM) de volgende van toepassing:
- Algemene Verordening Gegevensbescherming (AVG of GDPR) (2, 8)
- Electronic Identification Authentication And Trust Services (eIDAS)
- Wet algemene bepalingen burgerservicenummer (11)
- Wet elektronisch bestuurlijk verkeer (12)
- Algemene wet bestuursrecht (3)

De wet Wet electronische handtekening (13) is inmiddels vervangen door de Europese eIDAS verordening. Daarmee is een wettelijk kader voor betrouwbaarheidsniveaus geschapen dat direct relevant is voor IAM. Dit wettelijke kader omvat eisen aan authenticatiemiddelen en IAM processen[1].

Daarnaast zal de wet Digitale Overheid (WDO) algemene verplichtingen omtrent informatiebeveiliging zoals het voldoen aan de BIO en de DigiD beveiligingsrichtlijnen een directe wettelijke basis geven. Deze regels gelden echter nu ook al voor bijvoorbeeld OLO2 op grond van de lagere regelgeving.

Voor de wet Digitale Overheid (WDO) geldt dat deze op dit moment nog geen onderdeel is van het wettelijk kader echter zeer waarschijnlijk wél voor ingangsdatum van de Omgevingswet en daarmee tevens kaderstellend. Deze zal de toepassing van GDI componenten (Generieke Digitale Infrastructuur) voor authenticatie in DSO verplicht maken waaronder inlogmiddelen van private partijen.

Deze eisen uit wet- en regelgeving zijn zodanig dat gesteld kan worden dat Toegang middels IAM deel uitmaakt van het “robuuste” deel van het stelsel (zie doelarchitectuur § 4.1).

[1] Meer info over deze eisen, zie Handreiking betrouwbaarheidsniveaus versie 4 www.forumstandaardisatie.nl/thema/handreiking-betrouwbaarheidsniveaus

2.2 *Principes*

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

Voor elke principe dat van toepassing is, wordt aangegeven hoe deze ingevuld wordt voor deze GAS. Om duplicatie van teksten in de OGAS te voorkomen worden op de identificatie, statement en eisen na de andere standaard onderdelen van een principe weggelaten. Hiervoor kan de OGAS geraadpleegd worden.

Identificatie	
Statement	Het stelsel functioneert als 1 geheel voor zowel personen als systemen.
Eisen	Eindgebruikers hoeven maar één keer in te loggen via het portaal. Gebruikersgegevens worden slechts op één plaats vastgelegd. Voorinvullen van persoonsgegevens geschiedt middels Basisregistraties.

Identificatie	
Statement	Alles is een service
Eisen	Toegang wordt geïmplementeerd middels toegangsservices die als API's op het Knooppunt ter beschikking worden gesteld. Koppelingen met externe Identity Providers (IdPs) verlopen conform de aansluiteisen van de betreffende IdP rechtstreeks met de DSO Identity Server (IS) Externe toegangsservices zoals die van het Centraal Aansluitpunt worden via het Knooppunt ontsloten.

Identificatie	
Statement	Oplossingen zijn eenvoudig, generiek en kosten effectief.
Eisen	IAM wordt (vrijwel) geheel ingevuld met GDI voorzieningen en standaard middleware en infrastructuur componenten (aangevuld met platformservices die door het Knooppunt geleverd worden). Voor ontbrekende functionaliteit in GDI voorzieningen worden geen tijdelijke alternatieven gerealiseerd.

Identificatie	
Statement	Hergebruik voor koop voor maak.
Eisen	Bij keuzes aangaande informatie-uitwisselingsstandaarden is niet alleen de formele standaard (SAML) het uitgangspunt maar ook de vraag welke delen daarvan "standaard" (plain vanilla) geleverd worden in relevante open source componenten en veel gebruikte componenten op de markt.

Identificatie	
Statement	Beheerfunctionaliteit is primaire functionaliteit.
Eisen	Voor de registratie en het beheer van IAM gegevens: identiteiten, authenticatiemiddelen van overige gebruikers, persoonsgegevens en machtigingen worden GDI componenten gebruikt.

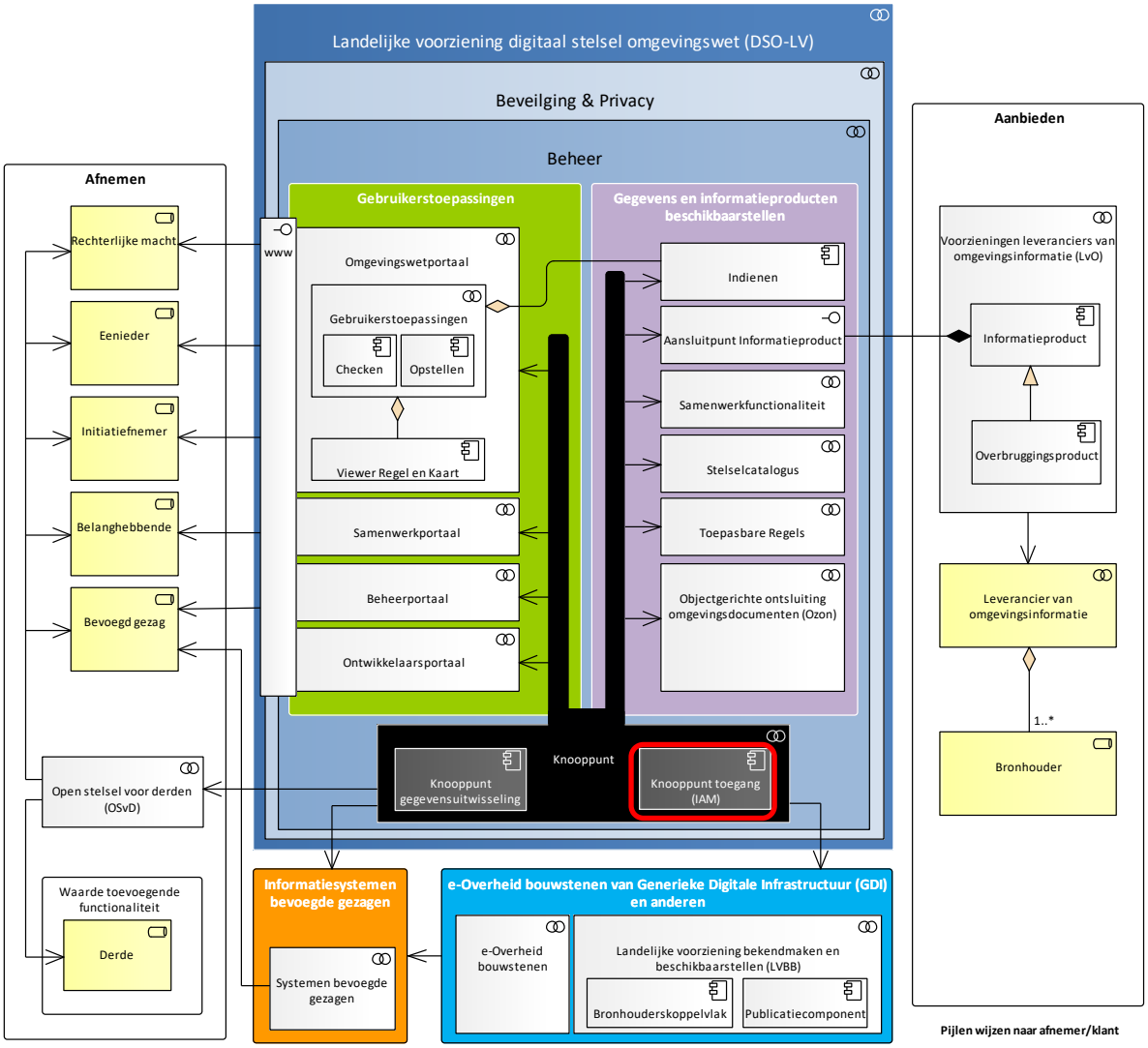
	Ook voor medewerkers van bevoegd gezag worden GDI componenten ingezet (eHerkenning).

Identificatie	
Statement	Passende beveiliging voor reële risico's.
Eisen	Om privacy inbreuken te beperken wordt het gebruik van persoonsgegevens zoveel mogelijk beperkt middels dataminmalisatie. O.a na inloggen wordt het BSN vervangen door een informatieloos pseudoniem, keuze van een eigen toonbare schermnaam, verwerking van persoonsgegevens alleen toe te staan als het een duidelijk doel dient en enkel aan gebruikers te tonen als dit nut heeft in de communicatie.

3 Organisatie

In dit hoofdstuk wordt de Organisatielaag beschreven van Knooppunt – Toegang (IAM), deze is bepalend voor de te kiezen oplossingen. Dit hoofdstuk positioneert de GAS in het stelsel, waarin de ketens uit de OGAS als basis zijn gebruikt. Er zijn geen afhankelijkheden van andere DSO-LV Componenten, wel van GDI eOverheidsbouwstenen

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

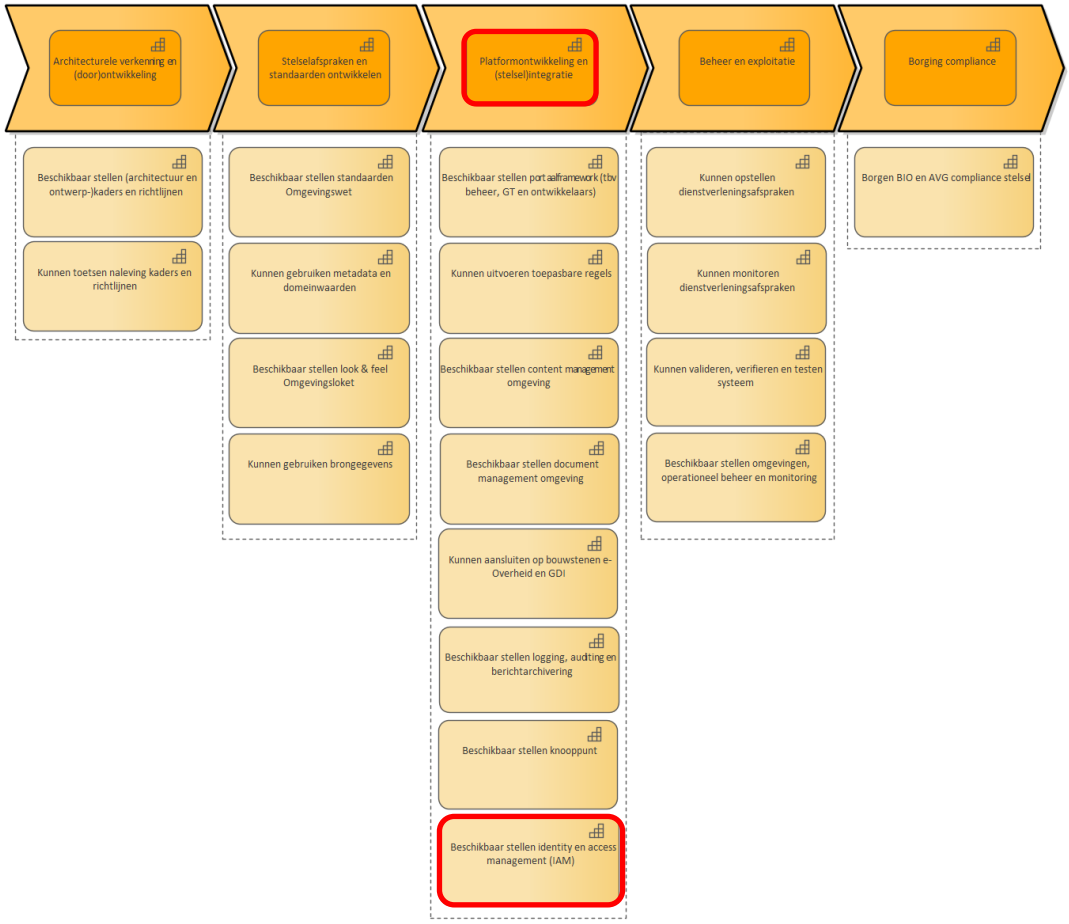


Figuur 1 – Positionering GAS

IAM is een randvoorwaarde bij het (veilig) uitwisselen van gegevens. IAM functionaliteit wordt binnen het Digitaal Stelsel Omgevingswet ingebouwd in het onderdeel Knooppunt. Gebruikers, gebruikerstoepassingen en de andere onderdelen van het stelsel benutten deze functionaliteit. IAM is ook een randvoorwaarde voor de inrichting en borging van beveiliging, privacy en beheer.

3.1 *Overzicht capabilities*

In deze paragraaf wordt de positionering en de context van Knooppunt – Toegang (IAM) t.o.v. van het gehele stelsel weergegeven. Het stelsel wordt hier beschouwd vanuit de relevante waardeketens en de bijbehorende specifieke capabilities.

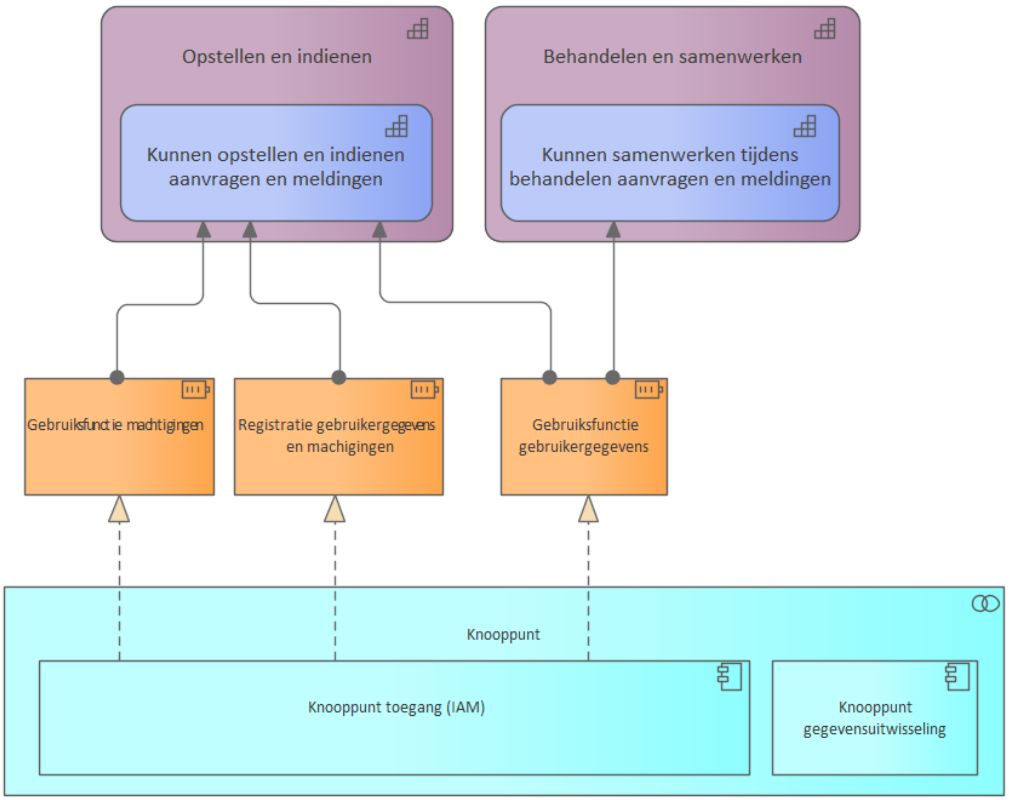


Figuur 2 – Ondersteuning capabilities in de keten "Behoefte tot Realisatie"

IAM is één van de enabling capabilities die het platform completeren en bijdragen aan de stelstelintegratie door de toegang aan de portaalkant te faciliteren en de verspreiding van identiteiteits- en rolgegevens binnen de componenten van DSO-LV.

3.2 *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 de componentcluster Knooppunt – Toegang (IAM) binnen DSO-LV. Deze zogenaamde toewijzing vanuit de voorziening is gevisualiseerd in Figuur 3.



Figuur 3 – Resources toegewezen aan capabilities

Om IAM te kunnen gebruiken is voorafgaande registratie nodig. Voor IAM worden overheidsbrede GDI-bouwstenen[2] gebruikt. De meeste gebruikers zullen zich daar registreren. Dit gaat buiten DSO om en vraagt dus geen registratiefuncties vanuit DSO. Alleen voor de restgroep die niet over een GDI verstrekt middel kan beschikken zal binnen DSO een eigen registratie en identity provider wordt ingericht.

Knooppunt Toegang (IAM) zal onderverdeeld zijn in toegangsservices voor registratie en gebruik van inloggen/toegang/machtigingen voor Burgers, Bedrijven, Bevoegd Gezagen, overige DSO-gebruikers en middels Apps via het Open Stelsel. Daarnaast roltoekenning voor autorisatie en personaliseren vóór inloggen.

#	Resource	Toelichting

[2] In het vervolg worden de huidige GDI voorzieningen als DigiD en eHerkenning genoemd. In kader van eID stelsel, eIDAS en ETD ontwikkelen deze zich. DSO zal deze ontwikkeling volgen.

	Registratie gebruikersgegevens en machtigingen	Voor het kunnen gebruiken van gebruikersgegevens en machtigingen dienen de identiteiten en machtigingsrelaties geregistreerd te worden. Dit zal meestal een externe registratie zijn.
	Gebruik Gebruikersgegevens	De identiteiten, rollen en bijbehorende profielgegevens kunnen samen met aan deze identiteiten gerelateerde gegevens uit externe registraties (zoals BRP) worden gebruikt voor authenticatie, autorisatie en voorinvullen van persoonsgegevens.
	Gebruik Machtigingen	Indien een initiatiefnemer een machtiging heeft afgegeven aan een persoon of organisatie zal deze persoon of medewerker namens of in de plaats van de initiatiefnemer rechtshandelingen uitvoeren binnen de in de machtiging beschreven bevoegdheid.

Alle onderdelen van deze abstracte resources worden als individuele Toegangsservices gepositioneerd (zie H5).

3.2.1 *Welke identiteiten c.q. actoren zijn relevant*

Alle bij DSO betrokken partijen moeten ondersteund worden en daarom zijn alle in de DSO visie onderkende afnemers, gebruikers en aanbieders ook IAM actoren.

IAM identificeert partijen via de individuele eindgebruikers en systemen waarmee deze partijen diensten afnemen (c.q. aanbieden). Voor een burger vallen deze samen met de juridische partij, voor bedrijven, organisaties en overheden geldt dat niet. Daar omvat één juridische partij mogelijk vele individuele eindgebruikers. Evenzeer kunnen vele verschillende systemen onder verantwoordelijkheid van één partij vallen.

Technisch gesproken kan gebruik van DSO alleen aan deze partijen toegerekend worden door het gebruik van de individuele eindgebruikers die namens hen handelen te volgen binnen de DSO voorzieningen. Deze toerekening is noodzakelijk om aan de wettelijke eisen te voldoen en conform "informatieveiligheid en privacybescherming zijn noodzakelijk" [D4]. Voor berichtenverkeer met systemen moet gelogd worden welk bericht van welk systeem afkomstig is en zijn er afspraken met de verantwoordelijke voor die systemen.

Naast de afnemers, gebruikers en aanbieders vormen ook de DSO-beheerders een groep voor IAM relevante partijen (GpvE § 2.8). DSO-beheerders zijn medewerkers van de beheerorganisatie DSO die toegang hebben tot het DSO-platform en bijbehorende OTAP-straat en voorzieningen. Juridisch gesproken vallen zij onder verantwoordelijkheid van de stelselbeheerder.

Tenslotte wordt in de visie en doelarchitectuur over derden gesproken, te weten software-leveranciers en app ontwikkelaars. App ontwikkelaars zijn partijen die het open deel van DSO benutten om daarmee hun eigen producten te ontwikkelen. Dit kunnen zowel individuen als medewerkers van software bedrijven zijn. De term software leveranciers wordt tevens gebruikt voor partijen die in opdracht van bevoegd gezagen software ontwikkelen. Een scherp onderscheid is er niet. Het komt voor dat bevoegd gezag deze software als cloud oplossing gebruikt zodat technisch gesproken

deze software leveranciers in opdracht van bevoegd gezagen gegevens uitwisselen met DSO.

In de visie en doelarchitectuur worden deze verschillende doelgroepen globaal aangeduid. Voor IAM worden ze als volgt opgevat.

Actor	**Natuurlijk persoon**	**Medewerker van**	**Opmerkingen**
Gebruikers			Onder Gebruikers worden de onderstaande doelgroepen verstaan. Gebruikers zijn afnemers van DSO diensten.
Eenieder	Kan	Kan	Eenieder moet de mogelijkheid hebben de open informatie en services van DSO te gebruiken. Hiervoor is het niet nodig dat DSO juridische zekerheid heeft wie het betreft. Personalisatie is wel mogelijk.
Initiatiefnemer	Kan	Kan	Zodra initiatiefnemers een aanvraag of melding indienen moeten er voldoende betrouwbaar juridisch vast liggen wie het betreft (welke burger of rechtspersoon het is). Al eerder in het proces is personalisatie mogelijk. De initiatiefnemer kan eerder beslissen zich bekend te maken en in te loggen. Vanaf dat moment kan DSO zijn gegevens betrouwbaar afschermen van anderen.
Belang-hebbende	Kan	Kan	Van een belanghebbende moet voldoende betrouwbaar juridisch vast liggen wie het betreft. Anonieme belanghebbenden bestaan niet. Alleen aan identificeerbare belanghebbende kan toegang gegeven worden tot gegevens over een bepaalde zaak.
Bevoegd Gezag	Nee	Altijd	Alle processtappen die Bevoegd Gezag uitvoert vereisen dat vastligt welk Bevoegd Gezag het betreft. Vanuit informatie-beveiligingseisen geldt dat daarbij op medewerker niveau gelogd wordt wie wat doet. Dat wil overigens niet zeggen dat anderen moeten kunnen zien welke medewerker welke handeling verricht heeft.
Rechterlijke macht	Nee	Altijd	Op dit moment geen afzonderlijke groep omdat er geen aparte requirements bekend zijn. Zie uitleg hieronder.
Andere afnemers			Naast Gebruikers zijn er de onderstaande andere afnemers, ook wel aangeduid als “derden”.
Software-leverancier	Kan (?)	Kan	Dit betreft makers en leveranciers van software voor DSO gebruikers. Zij kunnen deze software aanbieden als cloud dienst in opdracht van een bevoegd gezag (zie KPN02). Er is geen wezenlijk verschil met app bouwers.
App bouwers	Kan	Kan	Dit betreft afnemers van de open gegevens en services van DSO. Hun apps maken gebruik van

			deze gegevens en services, het kan zijn dat Gebruikers zich via deze apps authenticeren. Daarnaast zijn App bouwers actor bij het aanmelden van nieuwe (versies) van hun app. In dat proces wordt de authenticatie van de app binnen DSO vastgelegd. Er is geen wezenlijk verschil met software leveranciers.
Overige actoren			Onderstaande actoren zijn ook van belang voor DSO IAM.
Stelselverant-woordelijke	Nee	Altijd	De stelselverantwoordelijke heeft een eigen identiteit. Afnemers van diensten moeten immers zeker zijn dat diensten daadwerkelijk van DSO afkomstig zijn. Indien dit een collectief van overheden wordt, dan zal ergens vast moeten liggen welke partijen het omvat. Deze stelselverantwoordelijke richt een DSO-beheerorganisatie in welke de tactische en operationele beheerverantwoordelijkheid voor DSO uitvoert
DSO-beheerder	Altijd	Altijd	Een individuele medewerker van de DSO-beheerorganisatie. Voor het beheer van DSO worden dezelfde IAM voorzieningen benut, mogelijk aangevuld met infrastructurele beveiligingsmaatregelen.
Aanbieder	Nee	Altijd	Dit betreft (semi-)publieke organisaties, bijvoorbeeld informatiehuizen en ontwikkelpartners als RWS en Kadaster die informatie/functionaliteit binnen het DSO aanbieden.

N.B. In de visie (§3.1, wordt de rechterlijke macht als een afzonderlijke doelgroep genoemd. In GpvE en andere stukken worden voor deze groep echter geen andere eisen gesteld dan wat al geldt voor belanghebbenden, namelijk de mogelijkheid om gegevens van een bepaalde zaak enkel toegankelijk te maken voor een beperkte groep. Het kan zijn dat dit in het kader van verdere uitwerking van de eisen vanuit vergunning, toezicht en handhavingsprocessen nog verandert. Voor dit moment wordt aangenomen dat er geen aanvullende eisen zijn.

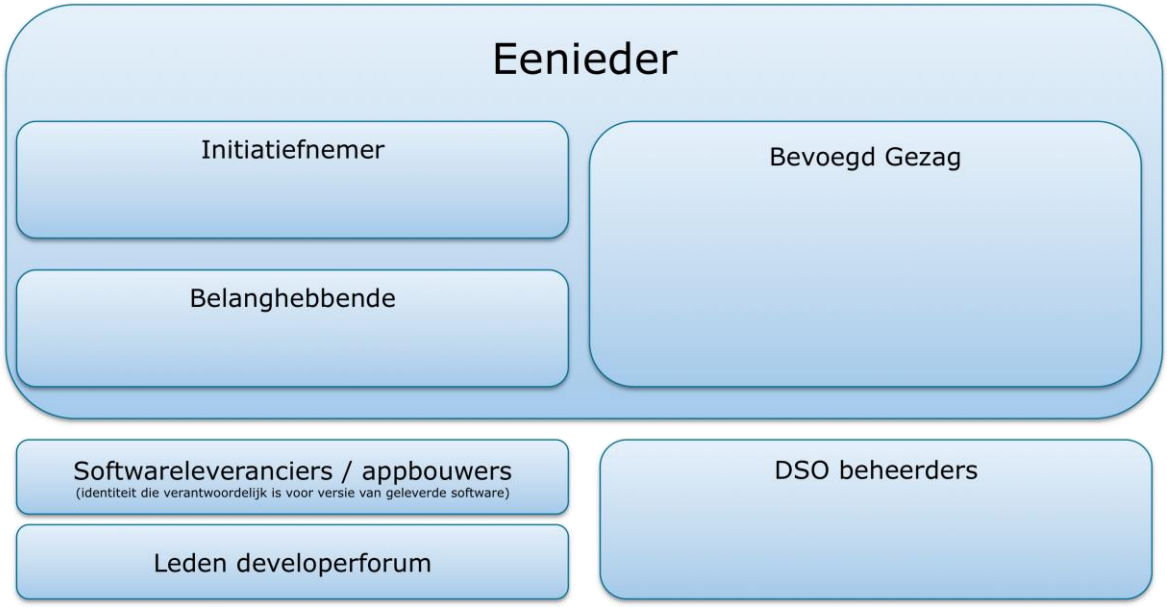
3.2.2 *Verschil in rol*

Dezelfde partij kan voorkomen als verschillende van bovengenoemde actoren (in de tabel). De medewerker van een bevoegd gezag kan bijvoorbeeld belanghebbende zijn inzake een situatie in zijn woonbuurt. Een software-leverancier kan los van zijn rol als software-leverancier initiatiefnemer zijn etc. Een overheidsorganisatie die optreedt als bevoegd gezag kan in andere rol zelf initiatiefnemer zijn of belanghebbende. Ook kan iemand eerst DSO gebruiken als eenieder, enkel ter oriëntatie en zich pas verderop in het ketenproces kenbaar maken als initiatiefnemer of belanghebbende.

In het algemeen wordt dit in IAM architecturen opgelost door de partij en diens rol, dat wil zeggen de hoedanigheid waarin de partij handelt, te scheiden. De partij wordt

dan op basis van één middel geauthenticeerd (wie je bent) en de rol bepaalt de autorisaties (dat wat je mag) in de betreffende situatie. Voor de DSO is deze algemene oplossing echter niet helemaal geschikt. Dit omdat er situatie zijn waarin het voor zo'n partij gewenst kan zijn voor heel verschillende rollen, verschillende typen authenticatiemiddelen toe te passen. Of – van de kant van DSO gezien – er geen (juridische) reden is om het feit dat achter de ene en de andere rol dezelfde partij schuil gaat, vast te leggen.

Dit is het beste te illustreren met Venn-diagrammen c.q. verzamelingen. De verzameling partijen kan als volgt in deelverzamelingen worden opgedeeld:

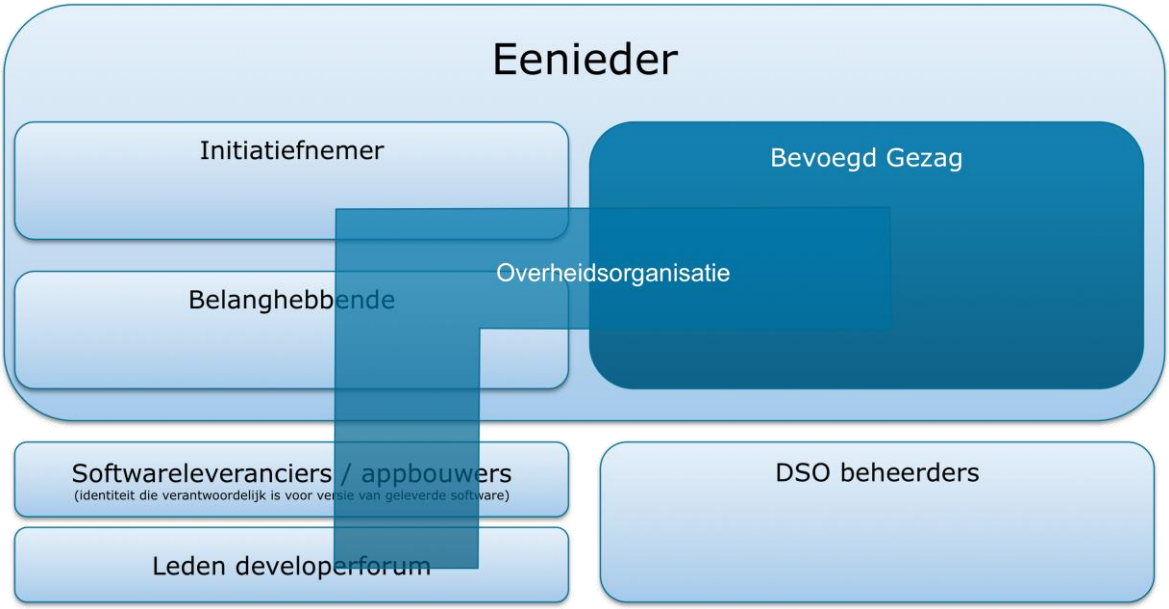


Het begrip "rol" wordt binnen het programma op verschillende manieren gebruikt. Er wordt gesproken over Gebruikers met verschillende rollen, wanneer bijvoorbeeld bedoeld wordt dat een gemeente (die meestal de rol bevoegd gezag heeft) ook zelf initiatiefnemer kan zijn. Er wordt gesproken over de verschillende rollen van bevoegd gezag, zoals planvorming, vergunningsverlening, toezicht en handhaving.

Deze uitwerking start met het principe dat voor IAM de actoren in bovenstaande doelgroepen los van elkaar staan. Dit echter met uitzondering van eenieder, belanghebbenden en initiatiefnemers. In het Venn-diagram is te zien dat deze samenhangen. Daar wordt het principe van naadloze gebruikerservaring gevolgd (§ 3.8 doelarchitectuur, LOK10). Een eindgebruiker, burger of bedrijf, kan DSO beginnen te gebruiken als eenieder zonder in te loggen. Vervolgens is het de keuze van de eindgebruiker of personalisatie wordt toegepast. Wordt de eindgebruiker verderop in het proces initiatiefnemer of belanghebbende (die een zienswijze wil indienen of samenwerken) dan is inloggen vereist. De eerdere personalisatie wordt "naadloos" overgenomen. De eindgebruiker kan ervoor kiezen eerder in te loggen. De mogelijkheid de eigen gegevens af te schermen is alleen beschikbaar nadat er ingelogd is en vanaf dat moment zijn betreffende gegevens zonder inloggen niet zichtbaar. In deze keten is er dus sprake van overgang van de ene groep actoren naar de andere (van eenieder, naar belanghebbende of initiatiefnemer). Globaal kan wel gesteld worden dat oriëntatie volledig open is, checken een proces is waar personalisatie al nut heeft en opstellen aanvraag / melding inloggen vereist. De

eindgebruiker bepaalt echter het moment van overgang en kan al eerder personalisatie toepassen of inloggen en van bijbehorende functies gebruik maken.

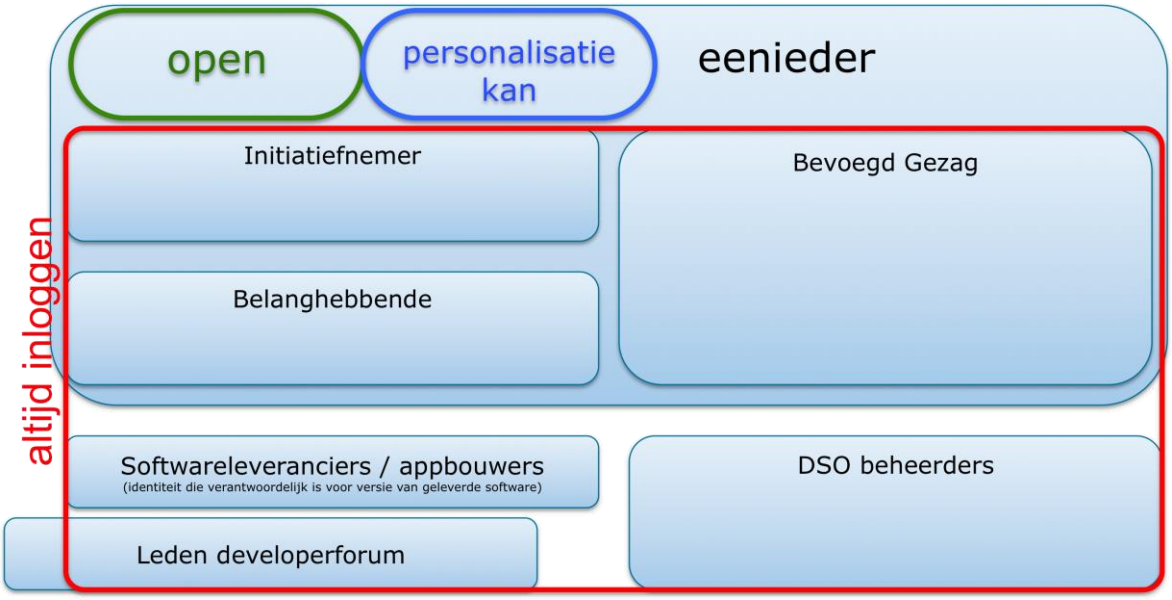
Een burger die apps bouwt zal in zijn hoedanigheid van app bouwer een andere identiteit hebben. Voor bijvoorbeeld een forum van app bouwers is het onnodig (en niet toegestaan) om eindgebruikers met hun BSN te identificeren. App bouwers c.q. software-leveranciers en leden van het developerforum vormen dus een aparte groep (en aparte deelverzamelingen in het Venn diagram).



Wanneer iemand als medewerker van bevoegd gezag of namens een bedrijf handelt dan is de machtiging[3] bepalend (machtiging wordt dus bewust gebruikt om preciezer te zijn dan de term "rol"). De machtiging bepaalt in welke groep de actor valt. De machtiging om als bevoegd gezag vergunningen te verlenen zal een andere zijn dan de machtiging om de gemeente als initiatiefnemer te vertegenwoordigen. Bevoegd gezag zal ook voor het proces oriënteren altijd ingelogd zijn en dan mogelijk meer gegevens zien. Het tweede Venn-diagram hierboven toont welke rollen een overheidsorganisatie kan spelen.

Samengevat: Er is een overzichtelijke afbakening van business rollen. Maar de manier waarop mensen en organisaties deze rollen vervullen varieert sterk. Er zijn allerlei combinaties mogelijk. De weergave van de doelgroepen voor IAM is daarom beter aan te duiden in de vorm van deelverzamelingen, zie volgende figuur:

[3] Voor precieze betekenis van "machtiging" en onderscheid met "autorisatie" zie begrippenlijst.



3.2.3 *Machtigingen*

Voor eenieder, initiatiefnemers en belanghebbenden geldt dat zij het recht (LOK18) hebben een ander te machtigen c.q. zich door een derde te laten vertegenwoordigen. Dit geldt zowel voor Burgers als voor Bedrijven.
Voor bevoegd gezagen geldt dat zij een andere overheidspartij kunnen mandateren om namens hen hun taak uit te voeren en/of in een Gemeenschappelijke Regeling kunnen samenwerken.
Voor alle situaties waar een medewerker namens een rechtspersoon gebruikt geldt dat ook sprake is van een machtiging. Ook de relatie tussen een systeem (een applicatie of service) en degene die ervoor verantwoordelijk is kan gezien worden als een machtiging.

Voor al deze situaties hanteren we de term “machtigen” als algemene term. Dit is in de eerste plaats een juridisch begrip.

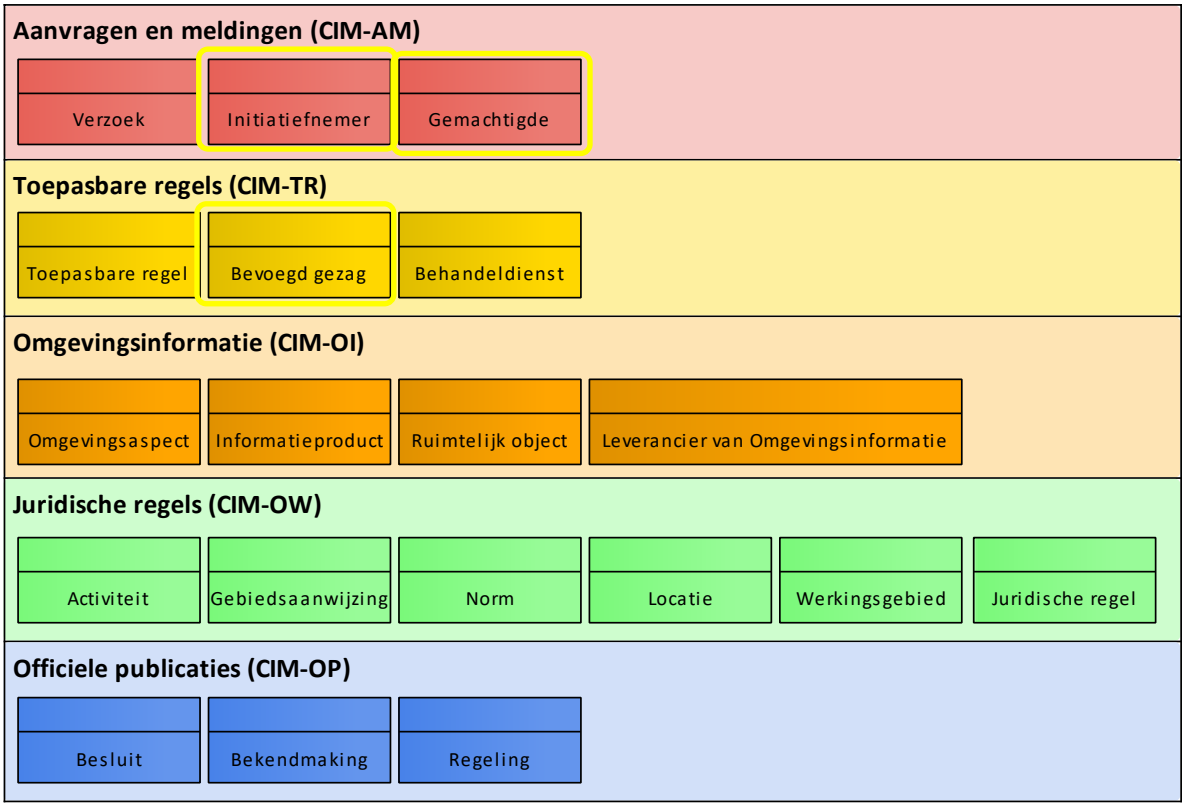
In principe worden de GDI voorzieningen voor machtigingen zo breed mogelijk toegepast. Dat betekent dat:

- Bevoegd gezagen eHerkenning toepassen. Iedere medewerker van een bevoegd gezag die DSO diensten benut moet voorzien worden van een eHerkenningsmiddel waarbij de machtiging om namens het bevoegd gezag te handelen wordt geregistreerd.
- Bedrijven, rechtspersonen en samenwerkingsverbanden passen eHerkenning toe. Iedere medewerker of bestuurder die namens deze partijen DSO diensten benut moet voorzien worden van een eHerkenningsmiddel waarbij de machtiging om deze partij te vertegenwoordigen wordt geregistreerd.
- Binnen Logius Machtigen en eHerkenning een grofmazige machtiging vastgelegd moet worden met de betekenis: “deze partij is gemachtigd mijn DSO zaken namens mij af te handelen”. De afbakening van deze machtigingen wordt bepaald door de afbakening van de diensten (en/of zaken) die vanuit DSO worden aangemeld bij Logius Machtigen, eHerkenning en/of DigiD. Dit geeft ruimte voor enige differentiatie in machtigingen.

4 Informatie

In dit hoofdstuk wordt de Informatielaag beschreven van Knooppunt – Toegang (IA) deze is bepalend voor de te kiezen oplossingen. In de OGAS is voor dit doel een globaal bedrijfsobjectenmodel (BOM) gepresenteerd.

In onderstaande figuur is met de rode omlijning weergegeven welke bedrijfsobjecten zich primair binnen het domein van Knooppunt Toegang (IAM) bevinden. Dit zijn er geen aangezien identiteiten en (natuurlijke en niet-natuurlijke) personen niet in het BOM terugkomen maar alleen in bepaalde rollen. Met de gele omlijning is aangegeven voor welke bedrijfsobjecten er sprake is van relaties/afhankelijkheden in aanliggende domeinen waar deze rollen weer terugkomen.



Figuur 4 – Bedrijfsobjectenmodel (BOM)

N.B. Behandeldienst is voor IAM geen (juridische) entiteit maar gemachtigde van het Bevoegd Gezag.

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 – Toegang (IAM).

4.1 *(bedrijfs)objectenmodel*

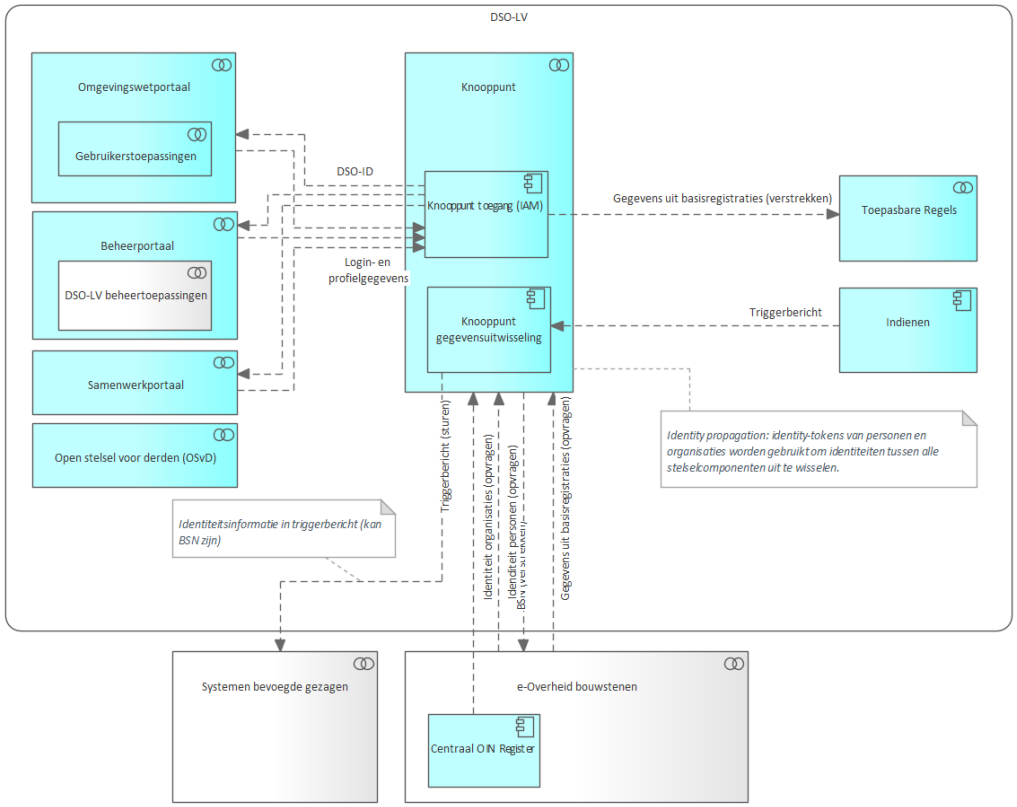
Deze paragraaf beschrijft de (bedrijfs)objecten die van toepassingen zijn voor deze GAS.

#	Bedrijfsobject	Toelichting
	Initiatiefnemer	Een Natuurlijk Persoon of een Niet Natuurlijk Persoon die het initiatief neemt tot fysieke ingrepen in de leefomgeving en daartoe een Verzoek bij het Bevoegd Gezag indient. (uit: IMAM)
	Gemachtigde	Een Natuurlijk Persoon of een Niet Natuurlijk Persoon die als vertegenwoordiger van een Initiatiefnemer optreedt. (uit: IMAM)
	Bevoegd Gezag	Het bestuursorgaan dat bevoegd is om ten aanzien van een Verzoek een besluit te nemen of een handeling uit te voeren. (uit: IMAM)

Zoals eerder aangegeven zijn er geen rode omcirkelingen in het BOM aangegeven aangezien in IAM de identiteiten en profielgegevens van natuurlijke personen worden beheerd die in een bepaalde context, meestal inloggen of machtigen, acteren in de hoedanigheid van initiatiefnemer, gemachtigde of medewerker van een bevoegd gezag.

4.2 *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 5 – Informatiestromen Knooppunt – Toegang (IAM)

Tussen alle componenten worden identiteitsgegevens uitgewisseld daar waar authenticatie, rollen voor autorisatie en voorinvullen van belang is. Soms zijn deze stromen meer functioneel zoals bij voorinvullen en soms vooral technisch zoals het uitwisselen van een identiteitstoken tussen IAM en een gebruikerstoepassing. Vanwege de vele verbindingen en abstractieniveau's zijn niet alle pijlen met de exacte IAM stromen getoond, maar zijn onderstaand de globale stromen weergegeven.

De globale informatiestromen lopen als volgt:

#	Informatiestroom	Van	Naar	Toelichting
1	Login en profiel gegevens persoon	Omgevingswet-Portaal Gebruikers-toepassingen	IAM	Voor authenticatie en aanpassing van bv email en telefoon wordt verstrekt door de persoon.
2	DSO-ID persoon	IAM	Omgevingswet-Portaal en Gebruikers-toepassingen	Na authenticatie wordt het pseudoniem van de persoon teruggegeven.
3	Login en profiel gegevens persoon	Beheerportaal Beheertoepassingen	IAM	Voor authenticatie en aanpassing van bv email en telefoon wordt verstrekt door de persoon.

#	Informatiestroom	Van	Naar	Toelichting
4	DSO-ID persoon	IAM	Beheerportaal Beheertoepassinge n	Na authenticatie wordt het pseudoniem van de persoon teruggegeven.
5	Login en profiel gegevens persoon	Samenwerkportaal	IAM	Voor authenticatie en aanpassing van bv email en telefoon wordt verstrekt door de persoon.
6	DSO-ID persoon	IAM	Samenwerkportaal	Na authenticatie wordt het pseudoniem van de persoon teruggegeven.
7	Identity propagation identity tokens van personen en organisaties	IAM	Alle stelsel componenten en Open stelsel voor Derden	Doorgeven van identiteiten van stelselcomponenten aan elkaar. Onder andere DSO_ID en DSO_ID van gemachtigde.
8	Identiteit personen	eOverheid (GDI IDP's)	IAM	Authenticatie en pseudoniem informatie Digid (BSN)/eHerkenning/eIDAS (*)
9	Identitorganisaties	eOverheid (COR)	IAM	Authenticatie informatie OIN
10	Basisgegevens Basisregistraties	eOverheid: BRP middels BSN NHR middels KvK	IAM	Voor in te vullen persoons en (bijbehorende) organisatie gegevens.
11	Basisgegevens Basisregistraties	IAM	Toepasbare regels	Voor in te vullen persoons en (bijbehorende) organisatie gegevens.
12	BSN	IAM	eOverheid: GDI IDP's, Machtigen en BRP	Verstrekken tbv authenticatie, machtigen en voorinvullen BRP.
13	Triggerbericht	Van Indienen via IAM	Systemen bevoegd gezag	Identiteitsinformatie in triggerbericht (kan BSN zijn)

(*) Exclusief DSO als IDP voor het eigen DSO Inlogmiddel

Zie de OGAS voor een nadere toelichting van de DSO-LV-componenten en de Landelijke componenten.

4.3 *Standaarden*

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

Forum Standaardisatie
De volgende standaarden van de lijst van het Forum Standaardisatie (http://www.forumstandaardisatie.nl) worden toegepast voor IAM:

Naam	Omschrijving	Bron	Beherende organisatie	Versie	Informatie

SAML	Security Assertion Markup Language	PTOLU	OASIS	2.0	T.b.v. uitwisseling van authenticatie- en autorisatietokens
https	Onderliggende standaard voor SAML		IETF	TLS 1.3	Ook TLS 1.2 geldig
ISO 27001 / 27002	Informatiebeveiliging. Van toepassing op toegangsbeleid	PTOLU	ISO / NEN	2013	In samenhang met de baseline BIO.
Digitale Toe-gankelijkheid (Webrichtlijnen)	Toegankelijkheid user interface	PTOLU	ETSI	EN 301 549	Wordt ook onderdeel van wettelijke GDI verplichting.
			W3C	WGAC 2.0	

Er zijn geen andere standaarden op de Pas-toe-of-leg-uit lijst met een voor IAM binnen DSO relevant toepassingsgebied. Bovengenoemde standaarden worden onderdeel van de wettelijke verplichting op grond van de wet GDI.

4.3.1 *Overige Standaarden*

Dit zijn aanvullende standaarden die niet bij het Forum Standaardisatie voorgeschreven worden, het betreft standaarden die voorkomen op de lijst van gangbare standaarden.

Naam	Omschrijving	Bron	Beherende organisatie	Versie	Informatie
XML	SAML is XML		W3C	1.1	
Oauth2	Voor authenticatie en autorisatie vanuit Apps		IETF	2.0	Nog in behandeling
OIDC	Voor authenticatie bovenop Oauth		OpenID Foundation	1.0	Nog in behandeling
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/

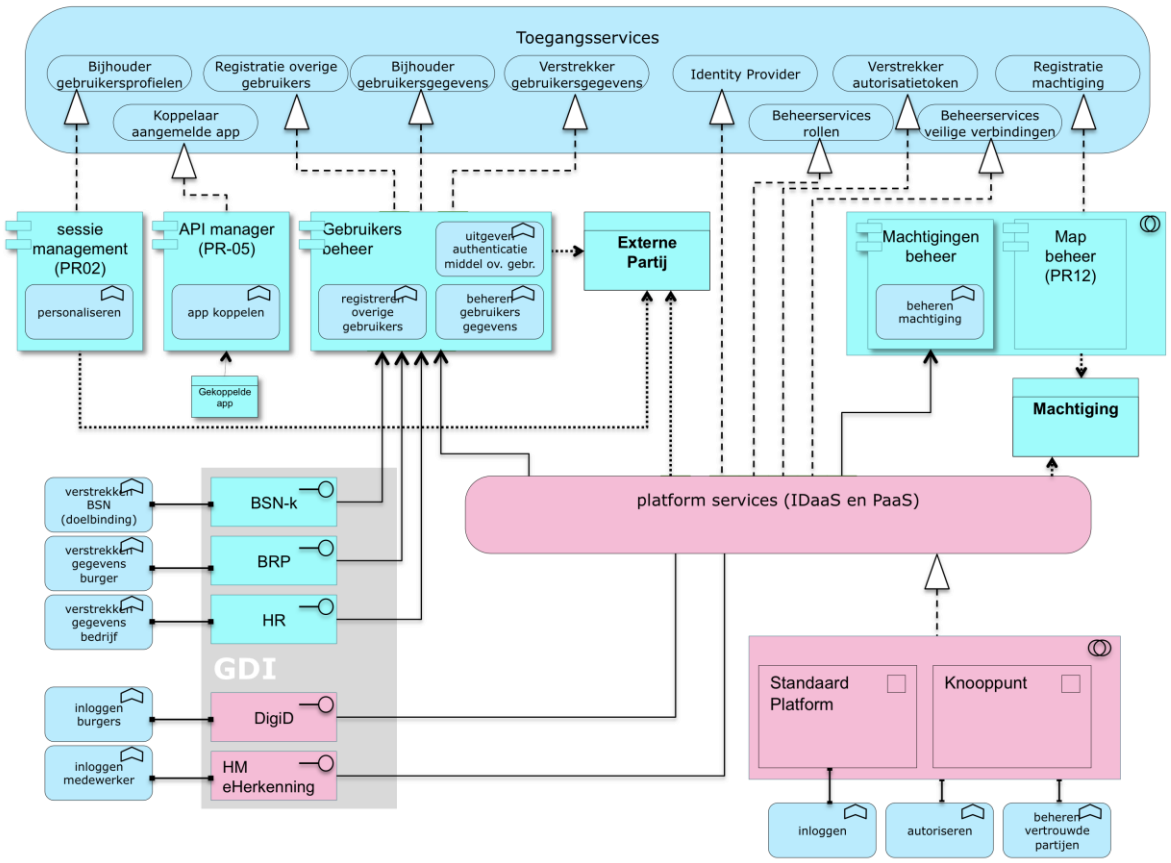
eHerkenning	Koppelvlak voor eHerkenning inlogmiddelen	Logius	eTD Afspraken-stelsel	1.11	
eIDAS	Koppelvlak voor EU inlogmiddelen	EU	EU	1.11	
ISO25010	Kwaliteitsstandaard met specifiek onderdeel beveiliging	ISO	ISO	2011	

5 Applicatie

In dit hoofdstuk wordt de applicatielaag beschreven van Knooppunt – Toegang (IAM), deze is bepalend voor de te kiezen oplossingen.

5.1 *Applicatie componenten*

Deze paragraaf beschrijft de applicatiecomponenten die van toepassingen zijn op deze GAS. Daarna worden de services beschreven die deze componenten aanbieden.



Figuur 6 - Applicatie-integratie Knooppunt – Toegang (IAM)

Legenda figuur 6: Roze = infrastructuurelementen (w.o. services en-interfaces), Blauw = applicatie elementen (w.o. componenten, functies, services en interfaces).

De applicatie componenten ondersteunen de realisatie van de Toegangsservices:

#	Applicatiecomponent	Toelichting
1	Sessiemanagement	De sessiemanagementcomponent regelt de technische connectie met een online gebruiker en is een voorwaarde voor inloggen. Daarnaast levert sessiemanagement ook de permalink en personalisatie op basis van b.v. cookies. Dat zijn vormen van herkenning van gebruikers die voorafgaand aan

		inloggen al voor kunnen komen. Bij inloggen moet de gebruikerservaring "naadloos" zijn en worden gepersonaliseerde gegevens dus hergebruikt. Alle informatie over de gebruiker wordt daarom als één object "DSO externe partij" gezien.
2	Gebruikersbeheer	De gebruikersbeheercomponent verstrekt informatie over ingelogde gebruikers. Indien mogelijk wordt deze informatie opgehaald uit de basisregistraties (zie de interfaces). Dat neemt niet weg dat er over alle gebruikers aanvullende gegevens kunnen worden vastgelegd. Voor overige gebruikers vindt ook registratie en middelenuitgifte plaats. Hoewel er meerdere typen gebruikers (burgers, bedrijven, bevoegd gezag etc.) zijn waarover gegevens bewaard worden, is de werking voor al deze typen gelijk.
3	Platformservices	De standaard IAM functies worden gerealiseerd door infrastructuurservices van het standaardplatform. Voor bepaalde functies werken deze samen met het knooppunt. Dit levert authenticatietokens en autorisatietokens conform de SAML of (voor apps) de OAuth standaard.
4	Machtigingenbeheer	Een component voor het toegankelijk maken en vastleggen van machtigingen in DSO kader.
5	API manager	Bij de API-manager worden (versies van) apps aangemeld / geregistreerd voor gebruik in DSO. De ontwikkelaar ontvangt daarbij een token dat in de app wordt opgenomen. De API-manager ondersteunt ook het koppelen van de app aan een eindgebruiker. OP runtime worden de tokens verwerkt door de platform services (identity server).

Vervolgens worden hieronder de services beschreven die deze componenten bieden.

5.2 *Toegangsservices*

#	Applicatiefunctie	Toelichting
1	Inloggen	Inloggen omvat het authenticeren voor alle typen eindgebruikers evenals het aanbieden van de keuzemogelijkheid aan eindgebruikers om aan te geven in welke hoedanigheid ze aanloggen en welk authenticatiemiddel ze wensen te benutten.
2	Inloggen Burgers	Interface naar DigiD
3	Inloggen Medewerker	Interface naar de eHerkenning herkenningsmakelaar. Het betreft medewerkers van zowel Bevoegd Gezag als van Bedrijven, andere organisaties en niet-natuurlijke personen.
4	Autoriseren	Dit omvat zowel het toekennen van rollen als standaardfunctionaliteit om een autorisatietoken te leveren als een standaardcomponent die in de applicatieserver een ontvangen autorisatietoken verifieert.
5	Registreren overige gebruikers	Voor gebruikers zonder DigiD of eHerkenning is een registratie nodig waarin gegevens over hen worden opgeslagen. Dit geldt zowel voor de restgroep als voor buitenlandse gebruikers die weliswaar via een eIDAS koppelpunt met het authenticatiemiddel dat ze in hun eigen land (EU) gebruiken kunnen inloggen, maar daarna toch gegevens zullen moeten registreren. DSO heeft namelijk geen

		toegang tot de basisregistraties van de betreffende andere landen.
6	Uitgeven authenticatiemiddel overige gebruikers	Na controle wordt aan overige gebruikers een DSO authenticatiemiddel verstrekt
7	Beheren gebruikersgegevens	Waar nodig worden gegevens over ingelogde gebruikers aan andere componenten doorgegeven. Daarmee wordt aan de eis voldaan dat gebruikers hun gegevens maar één keer aanleveren. Indien van toepassing kan doelbinding vanuit betreffende proces een voorwaarde zijn voor het benutten van gegevens zoals BSN en BRP-gegevens.
8	Beheren machtigingen	Verleende machtigingen moeten in elektronische vorm worden vastgelegd voordat ze benut kunnen worden.
9	Personaliseren	De functie om voorafgaand aan inloggen al comfortgegevens (bijvoorbeeld iemands naam zoals door hem of haar zelf opgegeven) over de gebruiker vast te leggen en de gebruiker in staat te stellen het proces te onderbreken en later zonder gegevensverlies te vervolgen.
10	Beheren vertrouwde partijen	Op diverse punten in de keten is vertrouwen in andere partijen essentieel. Dit wordt gecontroleerd op basis van o.a. PKIo certificaten. Er moet beheerd worden welke partijen op een bepaald moment "vertrouwd" zijn en welke certificaten benut worden om dat bij gebruik te controleren. Vertrouwde partijen omvatten zowel DSO interne partijen als DSO externe partijen waarmee berichtenverkeer plaats vindt als vertrouwde derden.
11	Koppelaar aangemelde app	Deze functie stelt gebruikers in staat om in te loggen en vervolgens een koppeling met een app tot stand te brengen, zodanig dat deze app daarna toegang heeft tot bepaalde gegevens die specifiek voor die gebruiker zijn. Dit doet een gebruiker eenmalig, daarna kan hij of zij zich authenticeren via de betreffende app. Het betreft enkel apps die al op basis van het binnen het knooppunt aanwezige mechanisme zijn aangemeld als DSO app.

5.3 *IAM specifieke koppelvlakken - SAML*

Voor IAM is de informatie-uitwisseling tussen de IAM voorziening en de componenten die IAM benutten het meest van belang. Deze informatie-uitwisseling vindt plaats op basis van de SAML-standaard.

Het authenticatie- en autorisatieproces kent globaal de volgende stappen:

1. Doorverwijzen eindgebruiker naar een identity provider. Per gebruikersgroep kan er onderscheid zijn of DigiD, eHerkenning of een andere identity provider relevant is.
2. Inloggen en authenticatie eindgebruiker bij de identity provider. De details hiervan worden bepaald door de Identity provider in kwestie.
3. Bepalen namens welke Gebruiker gehandeld wordt (bij een burger zonder machtiging vervalt die stap) en dit teruggeven aan het Bedrijfsproces dat de eindgebruiker wil doorlopen.
4. Doorgeven van de authenticatie in de verdere procesketen.
5. Controleren van toegang vanuit de verantwoordelijkheid van iedere losse schakel in de procesketen.

6. Indien nodig, bepalen en ophalen van nadere autorisaties
7. Indien nodig, ophalen van gegevens over de Gebruiker (need to know)

Daarbij wordt de volgende informatie uitgewisseld:

i. SAML authenticatierequest
iii. SAML authenticatieresponse
iv. en vi. SAML autorisatietoken
vii. Geen SAML. Bericht met gegevens over de gebruiker. Deze zijn via de service Verstrekken gegevens gebruiker afkomstig uit de eigen Gebruikers-GegevensService (GGS) of uit BRP of NHR. Daarbij kan het nodig zijn eerst het BSN op te halen via het BSN-koppelregister.

De berichten iii, iv en vi dragen bij aan privacy by design doordat zij geen privacy-gevoelige gegevens bevatten. Deze worden pas opgehaald in stap vii. Zo kan de controle of voldaan wordt aan de vereiste doelbinding specifiek gedaan worden. Privacy by default totdat doelbinding voor een bepaald proces is aangetoond.

Voor app toepassingen zal er een variant op dit proces zijn, gebaseerd op OAuth2.

5.4 *Herbruikbare bouwblokken*

In deze paragraaf worden de herbruikbare bouwblokken (benoemd in de OGAS) beschreven die van toepassing zijn voor deze GAS.

De herbruikbare bouwblokken zijn voor de realisatie van Toegang services middels IAM voornamelijk gericht op de GDI voorzieningen en basisregistraties die binnen dit domein van toepassing zijn.

#	Bouwblok	Type	Status	Toelichting
1	Logging, Auditing en Berichtarchivering	DSO	Beschikbaar	Onderdeel van Knooppunt Gegevens uitwisseling.
2	eOverheidsbouwstenen	GDI	Productie	Zie bij externe koppelvlak onder Netwerk
3	Beheer en Exploitatie	DSO	Inrichting	Alle enabling capabilities
4	Borging Compliance	DSO	Inrichting	Alle enabling capabilities

De volgende bouwblokken worden opgeleverd als herbruikbaar DSO bouwblok:

1	Gebruikersgegevens service (GGS)	IAM	Opgeleverd	Ophalen en opslaan van gebruikers- en profielinformatie in de IS (Identity Server).

n.b. Roltoekenning ten behoeve van autorisatie is geen herbruikbaar bouwblok maar integraal onderdeel van de (business-)logica van IAM.

6 Netwerk

In dit hoofdstuk wordt de Netwerklaag beschreven van Knooppunt Toegang (IAM), 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.

Voor het kunnen volgen van de ontwikkelingen op functionaliteit en standaarden/protocollen van Identity Access Management is het van belang een marktconforme Identity Server in te zetten.

6.2 *Aansluiting andere omgevingen*

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

#	Bouwblok	Type	Status	Toelichting
1	DigiD	GDI	Productie Logius	SAML versie.
2	eHerkenning / eIDAS	GDI	Productie	Vanaf versie 1.11
3	eID / eTD	GDI	Pilot	
4	BSN-koppelregister	GDI *)	Gerealiseerd	Voor private inlogmiddelen.
5	BRP service	BR/RvIG	Productie	Via Centraal Aansluitpunt IenM
6	NHR service	BR/KvK	Productie	Via Centraal Aansluitpunt IenM
7	eIDAS koppelvoorziening	GDI *)	Gerealiseerd	Voor EU birgers mét een BSN
8	PKIoverheid	GDI	Productie Logius	Ten behoeven van Digikoppeling en authenticatie organisaties.
9	Centraal OIN register (COR)	GDI	Opgeleverd Logius	
10	Machtigen	GDI	Realisatie Logius	Bevoegdheidsverklaringsdienst
11	BerichtenBox Burgers	GDI	Productie Logius	Onderdeel MijnOverheid
12	BerichtenBox Ondernemers	GDI	Planning	Onderdeel toekomstig Federatief Berichten Stelsel (FBS).

**) wordt in gebruik genomen op je moment dat de Wet Digitale Overheid in werking treedt.*

Aansluiting op externe GDI omgevingen zal in de toekomst vereenvoudigd worden.Door middels één aansluiting een reeks verschillende maar samenhangende diensten te kunnen afnemen. Een voorbeeld hiervoor zijn de authenticatie diensten , machtigen en portalen waarvoor Logius één zogenaamde Identity Bridge aan het realiseren is.

7 Beheer

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

IAM is onderdeel van de zorgplicht van de stelselorganisatie van het DSO. Vanuit verantwoordelijkheden bezien is het voor de werking van IAM dus noodzakelijk dat er één/een stelselorganisatie is aangewezen (conform APDSO01. "Eén stelselorganisatie voert regie op het digitaal stelsel.")

Omdat er sprake is van een stelsel houdt deze verantwoordelijkheid ook in dat alle gebruikers, aanbieders en afnemers gewezen worden op hun verantwoordelijkheden. Sommige aspecten van beveiliging vereisen dat gebruikers zich aan de regels houden en toezicht daarop vanuit DSO kan noodzakelijk zijn (zie visie D4 Informatieveiligheid en privacybescherming zijn noodzakelijk, LOK15). Wanneer een afnemer van DSO intern toestaat dat medewerkers elkaars wachtwoorden gebruiken dan kan DSO niet in haar verantwoordelijkheid voorzien dat ze weet welke gebruiker wanneer welke handeling verrichtte. IAM heeft dus organisatorische gevolgen. Deze beperken zich tot het invullen van een algemene verantwoordelijkheid die op grond van de baselines ook los van IAM al geldt.

Deze verantwoordelijkheid van de stelselorganisatie doet niets af aan de verantwoordelijkheid van iedere afnemer inzake beveiliging. Iedere afnemer beheert zelf machtigingen voor samenwerking, bedrijven en bevoegd gezagen zijn zelf verantwoordelijk voor hun eHerkenningsmiddelen en beheer van bijbehorende machtigingen. Voor beheer dienen bevoegd gezagen zelf verantwoordelijkheid te nemen voor het goed inregelen van beheermachtigingen. Waar nodig worden afnemers in gebruikersvoorwaarden op deze verantwoordelijkheden gewezen.

Daarnaast is er de specifieke organisatie van IAM. Hiervoor is de DSO beheerorganisatie verantwoordelijk. Deze omvat:

- Eigenaarschap van de IAM functies
- Verantwoordelijkheid voor relaties met GDI bouwstenen, zoals autorisatiebesluiten, gebruiksovereenkomsten, certificate policies PKIoverheid e.d.
- Organisatie van de supportlijnen naar achterliggende beheerpartijen in de IAM keten (zoals Centraal Aansluitpunt en Logius).

Het expliciet beleggen van deze verantwoordelijkheden is een voorwaarde voor BIO compliancy van de stelselorganisatie.

7.1 *Beheertoepassingen*

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

Voor beheer van persoonsgegegevens binnen de IAM context (profielen en identiteiten bij afloop van bewaartermijnen worden de standaard beheeronderdelen van de gekozen WSO2 Identity Server (IS) gebruikt.

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.

Aangezien IAM zelf een onmisbare schakel vormt in beveiliging en in het borgen van privacy wordt niet alleen ingegaan op de beveiligings- en privacy aspecten van IAM maar ook op de rol die IAM speelt in de beveiliging- en privacyborging van het gehele DSO.

De overall classificatie van IAM voorzieningen wordt bepaald door de overall classificatie van de andere DSO voorzieningen. Voor de delen van IAM waarin beheer van identiteiten en autorisaties plaats vindt is de classificatie minstens even hoog.

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*

De beschikbaarheid van alle producten die IAM gebruiksfuncties realiseren / het proces gebruiken IAM realiseren moet worden geclassificeerd als tenminste even hoog als de hoogste geclassificeerde toepassing die IAM gebruikt. Als de beschikbaarheid van IAM het laat afweten zal dit de beschikbaarheid van iedere component / toepassing die IAM nodig heeft raken.

Van de IAM registratiefuncties kan een lagere beschikbaarheid worden geaccepteerd. Dat neemt niet weg dat ook voor het kunnen aansluiten van nieuwe apps, voor het registreren van machtigingen etc. een hoge beschikbaarheid wordt verwacht die aansluit bij gebruikersverwachtingen (duidelijk meer dan kantoortijden).

In de volgende tabel wordt per bedrijfsservices de classificatie geduid waarbij afgeweken kan worden bovenstaande algemene insteek.

Component	Classificatie	Toelichting
Alle componenten die toegangsservices faciliteren.	Hoog	De hoogste huidige classificatie van een component die IAM benut.

8.1.2 *Integriteit*

De integriteit van het alle IAM functies en componenten moet worden geclassificeerd op de hoogste integriteitsclassificatie die binnen DSO voorkomt. Integriteit van "wie wat gedaan heeft" is een schakel in de gehele beveiliging en privacyborging. IAM mag niet de zwakste schakel zijn.

Bepaalde IAM gegevens zijn erg gevoelig voor gebreken in de integriteit. Voor deze gegevens zijn aanvullende integriteitschecks belangrijk:

- Unieke nummers
- Tokens
- Publieke delen sleutelmateriaal
- Certificaten
- Vastgelegde autorisaties

Deze gegevens worden grotendeels beheerd binnen het Knooppunt middleware platform en vallen dus onder de BIO compliancy daarvan. Alle bovengenoemde IAM gegevens worden in de componenten die toegangsservices benutten verwerkt op basis van ondertekende berichten, hetzij SAML tokens, hetzij certificaten. Als onderdeel van de secure coding richtlijnen dient zorgvuldige omgang met gegevens die uit deze beveiligde berichten komen te worden gecontroleerd.

Controle van de beveiligde berichten zelf vindt in principe weer plaats in applicatieservers binnen het platform. Waar dit uitbesteed is aan andere infrastructuren, ook voor wat betreft informatiehuizen, dient de verantwoordelijkheid voor deze controle te zijn overgedragen.

In de volgende tabel wordt per component de classificatie geduid waarbij afgeweken kan worden bovenstaande algemene insteek.

Component	Classificatie	Toelichting
Standaard platform infrastructuur	Hoog	Dit is strikt genomen geen "DSO" component maar een ingekochte component die wordt benut en waarvan DSO afhankelijk is.
Infrastructuren van DSO partners en informatiehuizen	Hoog	De classificatie en bijbehorende eisen vanuit DSO moeten opgelegd worden aan deze partners in de zin dat zijn verantwoordelijk moeten zijn voor controle van beveiligde berichten en veilige omgang met de daarin opgenomen gegevens.

8.1.3 *Vertrouwelijkheid*

De vertrouwelijkheid van de IAM functies en componenten betreft met name bepaalde gegevens(groepen). In IAM worden persoonsgegevens verwerkt. Als de vertrouwelijkheid het laat afweten is er al snel sprake van een datalek dat gemeld moet worden, bovendien vormt inbreuk in de vertrouwelijkheid van IAM gegevens een opzet naar andere inbreuken.

Gegevens	Classificatie	Toelichting
Persoonsgegevens algemeen	Midden	Er worden geen bijzondere persoonsgegevens verwerkt dus middel kan acceptabel zijn.
BSN	Hoog	Conform wettelijke grondslag.
Credentials die toegang geven tot gevoelige bedrijfsinformatie	Hoog	Betreft bedrijfsvertrouwelijke gegevens.

8.1.4 *Betrouwbaarheidsniveaus*

Uit bovengenoemde beveiligingsclassificaties van producten en gegevens in het DSO volgen de betrouwbaarheidsniveaus die gevraagd moeten worden voor de authenticatie van gebruikers. Op grond van eIDAS verordening zijn deze betrouwbaarheidsniveaus gestandaardiseerd op drie niveaus:

- Laag
- Substantieel
- Hoog

De criteria om het vereiste niveau te bepalen moeten toegepast worden op iedere DSO dienst afzonderlijk. Op grond van BSN verwerking in combinatie met andere persoonsgegevens en op grond van mogelijk economisch belang geldt voor een aantal DSO diensten en doelgroepen de classificatie Substantieel.

Wanneer deze toegepast worden op DSO dan leidt dit tot de volgende classificatie:

	Classificatie	Toelichting
Services voor Bevoegd Gezagen	Substantieel	Op grond van baseline is 2 factor authenticatie vereist.
Services voor samenwerking	Substantieel	Medewerkers bevoegd gezag.
Omgevingsloket	Laag tot Substantieel	Voor Gebruikers (Burgers en wellicht Bedrijven) die dat wensen moet Substantieel mogelijk zijn. Nader te bepalen of het vanuit DSO geaccepteerd wordt dat Gebruikers zelf voor lager betrouwbaarheidsniveau kiezen gezien het daaraan gekoppelde gebruiksgemak. Dit is een beleidsbeslissing.

Qua technische uitvoering moet het betrouwbaarheidsniveau als parameter worden doorgegeven zodat het mogelijk blijft diensten op een lager niveau aan te bieden en zodat – indien nodig – later ook een dienst op hoger betrouwbaarheidsniveau ingericht kan worden.

9 Transitie

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

Voor Digid wordt gestreefd naar betrouwbaarheidsniveau Laag (tot niveau substantieel onontkoombaar is). Single sign-on over GDI voorzieningen heen wordt op een later moment gerealiseerd.

Voor eIDAS zal vooralsnog alleen de minimaal wettelijk verplichte functionaliteit worden geïmplementeerd (Toegang voor EU burgers zonder BSN).

Private inlogmiddelen zullen pas na de inwerkingtreding van de Wet Digitale Overheid worden ondersteund waarna dit wettelijk verplicht is.

Het DSO pseudoniem (DSO-ID) is voorbereid op polymorfe pseudoniemen en het BSNk register.

Voor Machtigen zal periodiek de behoefte aan machtigingsfunctionaliteit en het aanbod van de in ontwikkeling zijnde functionaliteit op elkaar afgestemd worden om zo tot een voor DSO optimale invulling te komen. Dit geldt met name voor de zaakmachtiging.

N.B. Ook sommige externe registers en/of LvO's (Leveranciers van Omgevingsinformatie) zullen IAM benutten. Vanuit DSO worden kunnen namelijk gegevens worden opgevraagd waarvoor doelbinding of autorisatie voor een bepaalde burger of bedrijf vereist is. Om dit aan te tonen zal een DSO autorisatie doorgegeven worden (identity propagation). De betreffende partij moet de bijbehorende controles implementeren en geeft op basis van de van DSO ontvangen autorisatie toegang tot de gevraagde informatie.

Bijlage A: Bronnen

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

Interne bronnen:

Referentie	Document	Omschrijving
1	GAS Beveiliging Identity Access Management	0.53s
2	Notitie eIDAS toegang	0.9
3	Notitie Machtigen basisniveau DSO	0.4
4	Notitie DSO Organisatiegegevens	1.0

Externe bronnen:

Referentie	Document	Omschrijving

Bijlage B: Begrippen

Uit 'DSO - Architectuur - Afkortingen Begrippen' is slechts een beperkt aantal begrippen relevant, te weten:

Term	Definitie	Opmerking
Aanbieders	Aanbieders leveren gegevens of besluiten aan die via het DSO toegankelijk zijn. (§ 5.1.2 visie)	Het betreft o.a. bronhouders, beheerders overige registraties en generieke gegevensverzamelingen, informatiehuizen, zorgdragers
Afnemer	Afnemers van het Digitale Stelsel Omgevingswet. Doelarchitectuur § 5.1.2. stelt dat de afnemers onder te verdelen zijn in: - eenieder - initiatiefnemers - belanghebbenden - bevoegd gezagen	In visie is afnemer breder dan gebruiker, uitdrukkelijk incl. softwareleveranciers en andere derden (§5). In OGAS 1.34 is dat ook het geval: "Afnemers (binnen en buiten het stelsel) zijn gebruikers van het stelsel en/of ontwikkelen applicaties die services uit het stelsel afnemen. Afnemers zijn Eenieder (anonieme toegang), Initiatiefnemer, Belanghebbende, Bevoegd gezag, Derden en Rechterlijke macht." Term wordt ook benut in de definitie van dienst en in de zin van afnemer en aanbieder aan beide zijden van het stelsel/platform. Afnemers van DSO zijn dus bevoegd gezagen in hun rol in een keten, hun software leveranciers, derden die software maken etc.
Belanghebbende	Degene wiens belang rechtstreeks bij een besluit is betrokken.	Artikel 1:2 lid 1 Awb
Bevoegd gezag	Het bestuursorgaan dat bevoegd is een bepaald besluit te nemen of een handeling uit te voeren.	Artikel 1:1 lid 1 Awb
Derden	Softwareleveranciers die applicatie services van het stelsel afnemen. Dit kunnen leveranciers van app's zijn die waarde toevoegende diensten leveren of leveranciers van zaak systemen aan de bevoegd gezagen .	Zijn er nog andere derden dan softwareleveranciers en app bouwers, aangenomen wordt van niet. In § 3.1 van de visie worden derden en softwareleveranciers juist onderscheiden. Daar zijn de

	Omvat ook app bouwers, deze apps nemen immers applicatie services af.	softwareleveranciers als gemachtigden van b.v. bevoegd gezagen actief, daar betreft het een andere groep softwareleveranciers die uitvoerend optreden namens een overheidsorganisatie, veelal met een clouddienst.
Eenieder	Iedere persoon voor wie de Omgevingswet relevant is.	Personen met een andere rol zullen DSO soms ook als "eenieder" gebruiken.
Gebruiker	Gebruikers van DSO zijn eenieder, initiatiefnemers, belanghebbenden en bevoegd gezagen. Deze zijn onderscheiden van derden die onder het bredere begrip afnemer vallen en ook softwareleveranciers etc. omvatten.	Gebruikers zijn afnemers
Initiatiefnemer	Burgers, bedrijven en overheidsorganisaties die iets willen in de fysieke leefomgeving .	

Zie ook begrippen in 'Visie':

Begrip	**Toelichting**
Authenticatie	Authenticatie is het proces waarbij iemand nagaat of een gebruiker, een andere computer of applicatie daadwerkelijk is wie hij beweert te zijn. Bij de authenticatie wordt gecontroleerd of een opgegeven bewijs van identiteit overeenkomt met echtheidskenmerken, bijvoorbeeld een in het systeem geregistreerd bewijs. De authenticiteit van het object moet worden nagegaan. Een digitaal systeem met daarvoor ontworpen toepassingen kan hierbij helpen. Authenticatie volgt op identificatie, bij de voorbeelden aldaar: • Authenticatie is de controle dat een ingevoerd wachtwoord overeenkomt met het geregistreerde wachtwoord en hoort bij de opgegeven gebruikersnaam. • Authenticatie is dat een getoonde vingerafrduk overeenkomt met de geregistreerde vingerafdruk van de gebruiker. • Authenticatie is dat het door de token gegenereerde cryptografische geheim overeenkomt met het voor die token verwachtte geheim.
Autorisatie	Autorisatie is het proces onder verantwoordelijkheid van een dienstverlener waarin bepaald wordt of een subject (een persoon of een proces) toegang krijgt tot een object (een bestand, een systeem). Het subject kan daarbij een menselijke eindgebruiker zijn of een technisch systeem of proces.

	Bij autorisatie zijn twee partijen relevant: de dienstverlener en het subject. De verantwoordelijkheden liggen bij de dienstverlener, het betreft een proces dat zich afspeelt binnen deze dienstverlener. In een ICT voorziening wordt een autorisatie vastgelegd in toegangsrechten. Het verlenen van toegang zal gebaseerd zijn op de in toegangsrechten vastgelegde autorisatie. Het (vooraf) vastleggen van autorisatie is taalkundig moeilijk te onderscheiden van het moment waarop iedere keer dat de gebruiker de dienst benaderd gecontroleerd wordt of hij een geldige autorisatie bezit. Daarom is het voor dat laatste duidelijker te spreken over „toegang verlenen" of „een toegangsbeslissing nemen". Met verlenen van autorisatie bedoelen we dan het vastleggen van een autorisatie in toegangsrechten zodat deze steeds gebruikt kan worden.
Dienst	Een afgebakende prestatie van een persoon of organisatie (de dienstverlener), die voorziet in een behoefte van haar omgeving (de afnemers). [NORA]
Identificatie	Identificatie is het kenbaar maken van de identiteit van een subject (een gebruiker, gegeven of een proces) in de informatietechnologie. De identiteit wordt gebruikt in de vervolgstappen van IAM: authenticatie en autorisatie. Een object is bijvoorbeeld een computerbestand of een regel in een database. Identificatie kan op verschillende manieren plaatsvinden: in een inlogscherm invoeren van een gebruikersnaam, userid, DigiD, Idensys gebruik van een vingerafdruk of een ander biometrisch kenmerk gebruik van een token (een smartcard of een ander apparaatje, zoals een usb stick).
Identity Provider (Idp)	Een Identity Provider is een dienstverlener die de identiteit verifieert en authenticeert van een subject dat toegang wil verkrijgen en een bepaalde identiteit claimt.
Knooppunt	Een voorziening of organisatie die het afnemers makkelijk maakt aan te sluiten op beschikbare gegevensbronnen [NORA]
Machtiging	Machtiging is een herroepbaar recht van een persoon om een handeling te verrichten in naam van een andere persoon; een recht dat door deze ander (de vertegenwoordigde) verleend wordt aan eerstgenoemde persoon (de gemachtigde). Een machtiging kan algemeen of bijzonder zijn. Een bijzondere machtiging is beperkt tot bepaalde (rechts)handelingen of een bepaalde relevante omvang ten aanzien van (rechts)handelingen. Machtiging kan worden gezien als synoniem aan volmacht zij het dat de term machtiging voornamelijk in bestuursrechtelijke context wordt gebruikt.

	Machtiging is een meer juridisch begrip. Bij machtiging zijn drie partijen relevant: de vertegenwoordigde, de gemachtigde en derden (de dienstverlener). Het gaat om de verantwoordelijkheden van vertegenwoordiger en gemachtigde. Voor derden „maakt het niet uit" wie van beiden een dienst afneemt, zolang vertegenwoordiger en gemachtigde het onderling geregeld hebben. De focus van de verantwoordelijkheden ligt dus heel anders dan bij autorisatie. Nota bene: als de vertegenwoordigde dezelfde partij is als de dienstverlener dan lijkt een machtiging heel erg op een autorisatie. Dat is het geval wanneer een organisatie een medewerker machtigt. Juridisch is die machtiging vaak impliciet, maar in het geval van een formele mandateringsstructuur is het juist heel expliciet. De autorisatie is dan het technische effect in een ICT systeem van een machtiging. Maar een machtiging van een niet digitaal vaardige burger aan een familielid is een voorbeeld waar machtiging die duidelijk onderscheiden is van autorisatie.
Partij	Natuurlijk persoon, rechtspersoon of samenwerkingsverband van personen. In de DSO context zijn o.a. Aanbieders, Afnemers, Derden, Verstrekkers en de DSO Stelselverantwoordelijke partijen.