

Voorziening machtiging

Architectuur bij gemeenten

Inhoudsopgave

1. Inleiding.....	3
2. Bedrijfsarchitectuur.....	5
2.1. Doelen	5
2.2. Bedrijfsarchitectuur landelijk	6
2.3. Bedrijfsarchitectuur gemeentelijk.....	7
2.4. Conclusies	10
3. Informatiearchitectuur	12
3.1. Informatiearchitectuur landelijk	13
3.2. Informatiearchitectuur gemeente.....	15
3.3. Leveren van gemachtigde diensten	21
4. Technische architectuur.....	24
5. Machtigen in het vijf-lagenmodel	25
Bijlage 1: System-to-system en baliemachtigingen.....	28
Bijlage 3: Voorbeeld use cases	29

1. Inleiding

Er zijn veel situaties waarin burgers en bedrijven in Nederland behoefte hebben aan een verbeterd stelsel voor digitale machtigingen. Het nieuwe 'Stelsel van vertegenwoordiging' moet zorgen voor meer gebruiksgemak en rechtmatigheid – met daaruit volgend toenemende inclusie – maar ook minder regeldruk. Vooral door een efficiënter registratieproces voor gebruikers en voordelen bij bestuursorganen in hun primaire processen.

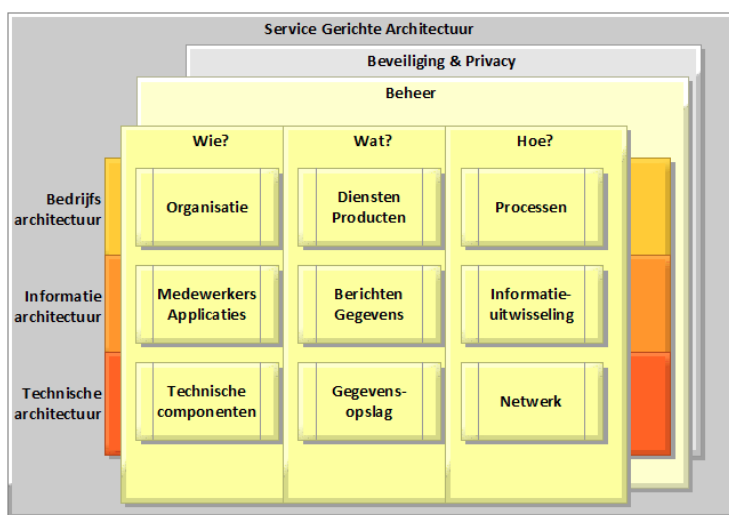
De VNG-notitie 'Handreiking Stelsel van vertegenwoordiging' bevat actuele informatie over de ontwikkeling van het nieuwe stelsel van vertegenwoordiging en de manier waarop gemeenten hier op kunnen gaan aansluiten. De handreiking geeft gemeenten inzicht en ondersteunt bij de implementatie van het stelsel.

Deze notitie beschrijft, aanvullend op de handreiking, hoe het stelsel past binnen de voor gemeenten geldende architectuur en binnen een aantal lopende ontwikkelingen zoals:

- het door gemeenten collectief ontwikkelen van voorzieningen via *Samen Organiseren*
- de *Gemeentelijke Model Architectuur (GEMMA)*
- de ontwikkeling van de *GEMMA-Gegevenslandschap* architectuur, en het in lijn daarmee
- realiseren van een nieuwe type informatievoorziening door de *Common Ground* beweging.

Doel is om duidelijk te maken hoe de gemeentelijke bedrijfsvoering en informatievoorziening in lijn met bovenstaande architectuur en ontwikkelingen geschikt is te maken om optimaal van het stelsel gebruik te kunnen maken.

De notitie bevat hoofdstukken over 'bedrijfsarchitectuur', 'informatiearchitectuur' en een (kort) hoofdstuk over 'technische architectuur'. In onderstaande afbeelding is binnen het NORA-negenvlaksmodel aangegeven wat globaal tot de verschillende typen architectuur wordt gerekend.



De notitie heeft als doel om een aantal architectuur-gerelateerde zaken te beschrijven die samenhangen met het (gaan) aansluiten op het stelsel van vertegenwoordiging. Daarbij wordt gebruik gemaakt van, in de Archimate-taal beschreven, architectuurdiagrammen. Die brengen een aantal kenraken in beeld via een een vereenvoudigde weergave waarin bewust bepaalde onderdelen en details zijn weggelaten.

Veel diagrammen hebben betrekking op de situatie waarin een gemachtigde namens een belanghebbende een gemeentelijke dienst wil aanvragen. Uiteraard zijn er meer situaties waarin machtigingen een rol spelen maar we gebruiken juist deze situatie als voorbeeld omdat het de eerste, en vaak voorkomende, processtap is waarbij gemeenten te maken krijgen met het willen gebruiken van een machtiging.

2. Bedrijfsarchitectuur

2.1. Doelen

Het stelsel van vertegenwoordiging wordt ontwikkeld vanuit een brede blik op enerzijds waar burgers en bedrijven (verder genoemd: 'gebruikers') behoefte aan hebben en anderzijds hoe bestuursorganen praktisch invulling kunnen geven aan de eisen die aan gebruik van het stelsel verbonden zijn.

Bij toepassing van machtigingen kan een gebruiker de rol van 'gemachtigde' of 'belanghebbende' hebben. De gebruiker in de rol van gemachtigde is gerechtigd om bepaalde acties namens de belanghebbende uit te voeren op basis van vrijwillige machtiging of wettelijke vertegenwoordiging. Het stelsel van vertegenwoordiging, en daarmee in lijn dit document, beperkt zich nu tot gebruik van machtigingen door burgers en bedrijven. Gebruik van machtigingen door systemen ('system to system') vallen hier vooralsnog buiten.

De op dit moment in gebruik zijnde voorzieningen om te kunnen machtigen zijn:

1. onvolledig (bijv. cliënten kunnen hun bewindvoerder niet machtigen)
2. versnipperd (er zijn verschillende, los van elkaar functionerende, machtigingsvoorzieningen)
3. niet-eenduidig (bijv. gemeenten bieden via eHerkenning te machtigen diensten op verschillende manieren aan)
4. gebruikersonvriendelijk (bijv. DigiD Machtigen is zodanig complex in gebruik dat slechts weinig mensen er gebruik van maken).

Het nieuwe stelsel van vertegenwoordiging wordt:

1. volledig (alle soorten machtigingen waar behoefte aan is worden ondersteund)
2. consistent (machtigingen zijn effectief toe te kennen en aan elkaar gerelateerd)
3. eenduidig (vergelijkbare diensten worden hetzelfde aangeboden)
4. gebruikers-vriendelijk¹:
 1. betrouwbaar (transparant en met eigen controle)
 2. persoonlijke benadering (afgestemd op de omstandigheden van de gebruiker)
 3. gemak (gebruikers kunnen snel en eenvoudig machtigen en van machtigingen gebruik maken)
5. bestuursorgaan-vriendelijk (bestuursorganen kunnen gemakkelijk van het stelsel gebruik maken).

¹ De kenmerken 'vertrouwen', 'persoonlijke benadering' en 'gemak' als invulling van 'gebruikersvriendelijk' zijn overgenomen uit de landelijke interactiestrategie, 'een integrale visie op overheidsinteractie, aan gedeelde uitgangspunten'.

- *Gemachtigde*: de persoon of het bedrijf die namens een belanghebbende een dienst wil aanvragen
- *Belanghebbende*: de persoon namense wie een gemachtigde op basis van een machtiging mag handelen
- *Bestuursorgaan*: de overheidsinstantie die deelneemt aan het stelsel van vertegenwoordiging en bepaalde diensten aanbiedt waarbij machtiging mogelijk is
- *Stelselorganisatie*: de organisatie die verantwoordelijk is voor de centrale stelselvoorzieningen en de stelselafspraken.

De stelselorganisatie levert:

- diensten waarmee gemachtigden en belanghebbenden machtigingen kunnen beheren
- diensten waarmee bestuursorganen aan kunnen geven bij welke van hun diensten machtiging mogelijk is
- bevoegdheidsverklaringen aan de hand waarvan een bestuursorgaan kan vaststellen welke machtigingsrelaties er zijn.

Bestuursorganen zorgen bij aanvraag van een te machtigen dienst dat:

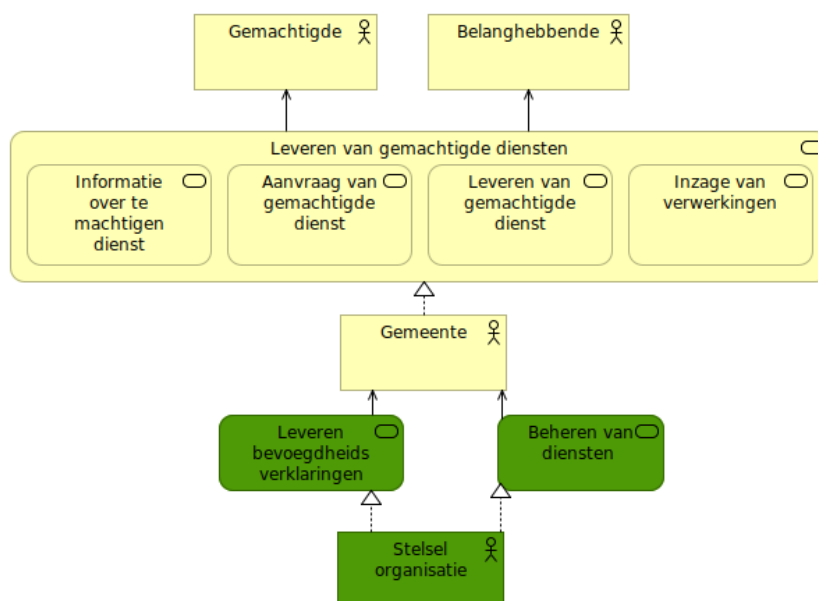
- de aanvragende gemachtigde wordt geauthenticeerd
- de BVD wordt gevraagd om de van toepassing zijnde bevoegdheidsverklaringen te leveren
- mede op basis van de verkregen informatie wordt beslist of de gemachtigde namens een belanghebbende een dienst mag aanvragen en de dienst vervolgens wordt geleverd.

Gemachtigden moeten:

- vooraf zorgen dat de benodigde machtiging aanwezig is
- zich authenticeren
- aangeven voor welke belanghebbende zij een dienst willen aanvragen
- na goedkeuring, de dienst namens de belanghebbende aanvragen.

2.3. Bedrijfsarchitectuur gemeentelijk

Gemeenten zijn een van de soorten bestuursorganen waarvan verwacht wordt dat zij bepaalde diensten 'machtigbaar maken'. Gebruikers kunnen vervolgens bij bezoek van een gemeentelijke website in de rol van gemachtigde gebruik maken van zo'n dienst namens een belanghebbende.



Het als gemeente 'leveren van gemachtigde diensten' bestaat uit een aantal deel-diensten:

- verstrekken van informatie over welke diensten via machtiging leverbaar zijn
- in staat stellen van een gemachtigde om dienst namens een belanghebbende aan te vragen
- leveren van de betreffende dienst aan de belanghebbende (en/of gemachtigde)
- bieden van inzage aan zowel belanghebbende als gemachtigde in opgetreden verwerkingen waarbij hun persoonlijke gegevens zijn gebruikt.

Op verschillende momenten, zoals bij de aanvraag, maakt de gemeente gebruik van door de stelselorganisatie geleverde bevoegdheidsverklaringen om (mede) op basis daarvan te bepalen welke acties mogen en moeten worden ondernomen.

In de volgende paragrafen wordt toegelicht hoe gemeenten het stelsel van vertegenwoordiging kunnen gebruiken in lijn met de uitgangspunten van achtereenvolgens Samen Organiseren, de GEMMA-referentiearchitectuur, het GEMMA-Gegevenslandschap en Common Ground.

2.3.1. Samen Organiseren

Iedere gemeente kan zelf bepalen welke te machtigen diensten, en in welke vorm, ze aanbiedt. Gelet op de doelen van het stelsel van vertegenwoordiging is het wenselijk dat gemeenten hierbij zoveel mogelijk standaardisatie nastreven. Gebruikers van het stelsel ervaren daardoor meer eenduidigheid en gemak en het wordt beter mogelijk om aanvraag en levering van diensten door gemeenten effectief op dezelfde manier uit te voeren.

In lijn met de doelen van Samen Organiseren is het de bedoeling om bij deze verandering zoveel mogelijk samen op te trekken en eenduidig vorm te geven aan hoe gemeenten aan het stelsel deelnemen. Gelet op het belang hiervan is het niet denkbeeldig dat in de toekomst het College van Dienstverleningszaken op onderdelen standaardisatie verplicht kan gaan stellen.

Belangrijkste aandachtspunten bij standaardisatie voor gemeenten zijn het gebruik van dezelfde diensten, diensten-sets en machtigingen, het gebruiken van dezelfde terminologie en het op vergelijkbare manier aanbieden van machtigingsmogelijkheden. In het hoofdstuk 'Informatiearchitectuur gemeenten' wordt beschreven hoe dit informatie-technisch is vorm te geven.

2.3.2. GEMMA-architectuurprincipes

De GEMMA-architectuurprincipes zijn richtinggevend en helpen gemeenten om goede keuzes te maken bij het inrichten van gemeentelijke processen en de informatievoorziening.

Principe	In relatie tot het stelsel
Onze gemeente denkt vanuit de positie van de klant	We machtigen diensten waar behoefte aan is bij klanten en bieden ze op een klantvriendelijke manier aan.
Onze gemeente gebruikt generieke processen en functies	We gaan gemachtigde diensten zoveel mogelijk op dezelfde manier aanbieden en leveren.
Onze gemeente voert regie over uitbestede diensten	Bij uitbesteding proberen we de manier van aanbieden en leveren zoveel mogelijk hetzelfde te houden.
Onze gemeente biedt de klant een goede informatiepositie aan	We informeren klanten over de mogelijkheid van machtigen en geven inzage in plaatsgevonden gebruik van machtigingen.
Onze gemeente digitaliseert haar diensten en processen	We digitaliseren diensten zodat het (ook) mogelijk wordt om ze via een gemachtigde aan te vragen.
Onze gemeente stelt openbare gegevens als open data beschikbaar	We publiceren (geanonimiseerde) gegevens over gebruik van machtigingen als open data.

Onze gemeente hergebruikt gegevens	We gebruiken uitsluitend binnen het stelsel vastgelegde informatie over diensten en machtigingen.
Onze gemeente gaat op een vertrouwelijke manier met gegevens om	We gaan vertrouwelijk om met machtigingen en bieden de mogelijkheid tot inzage in plaatsgevonden gebruik van machtiging ² .

2.3.3. GEMMA Gegevenslandschap

Het GEMMA Gegevenslandschap is een informatiearchitectuur voor gemeenten waarmee onder andere het scheiden van processen en gegevens mogelijk wordt en gegevens zoveel mogelijk 'uit de bron' worden gebruikt.

Principe	In relatie tot het stelsel
We werken met componenten	We voorkomen 'silo-systemen' maar gebruiken gemeentelijk herbruikbare componenten voor het omgaan met machtigen. Bijvoorbeeld door binnen de gemeente gebruik te maken van specialistische componenten voor autorisatie, logging en inzage.
We zijn transparant waar mogelijk	We laten zien waar machtigingen bruikbaar zijn en bieden inzage in gebruik er van. Bijvoorbeeld door gemachtigden en belanghebbenden inzicht te geven in verwerkingen waarbij relevante machtigingen zijn gebruikt.
We zorgen dat informatiebeveiliging en privacy op orde zijn	Bij gebruik van machtigingen hanteren we 'privacy by design en by default', houden we rekening met aanwezige doelbinding en leggen we verwerkingen vast in audit-logs. Bijvoorbeeld door aanvraag van diensten via machtiging niet toe te staan als er geen doelbinding is of als geen logging mogelijk is.
We leggen gegevens eenmalig vast en vragen op bij de bron	We gebruiken uitsluitend binnen het stelsel vastgelegde informatie over diensten en machtigingen en van informatie die beschikbaar is via GDI-bouwstenen. Bijvoorbeeld door zelf geen informatie ten behoeve van machtigen en authenticatie vast te leggen, maar gebruik te maken van stelselgegevens en voorzieningen zoals DigiD, eHerkenning en eIDAS-middelen.
We faciliteren regie op gegevens	We faciliteren gemachtigden en belanghebbenden om, via doorverwijzing, hun machtigingen te beheren en in te zien hoe er van machtigingen gebruik is gemaakt bij verwerkingen. Bijvoorbeeld door het opnemen van links naar centrale voorzieningen op de website en inzage via portaalvoorzieningen te ondersteunen.
We standaardiseren maximaal	We standaardiseren de manier waarop we als gemeenten machtigingen inrichten, aanbieden en gebruiken. Bijvoorbeeld door diensten(sets) en benodigde technische voorzieningen zoals een log-register te standaardiseren.

² Voor dit doel wordt onder andere een risicoanalyse door de Informatiebeveiligingsdienst uitgevoerd en wordt een Privacy Impact Assessment gedaan.

2.3.4. Common Ground

Common Ground is een beweging die een nieuwe type gemeentelijke informatievoorziening, in lijn met het GEMMA Gegevenslandschap, realiseert. Common Ground hanteert een aantal principes die richting geven aan hoe realisatie plaats vindt.

Principe	In relatie tot het stelsel
We werken als community	We werken samen met gemeenten en leveranciers en werken daarbij vanuit de gemeentelijke praktijk bij het bieden van de mogelijkheid om diensten te machtigen. Bijvoorbeeld door diensten en diensten-sets gezamenlijk te definiëren en vernieuwingen binnen de gemeentelijke informatievoorziening samen te ontwerpen en realiseren (bijvoorbeeld de manier van loggen en kunnen bieden van inzage).
We ontwikkelen incrementeel en iteratief	We werken agile, leveren met korte tussenpozen bruikbare (deel)producten op en leren van wat we doen. Bijvoorbeeld via proof-of-concepts en pilots.
We ontwikkelen nieuw naast bestaand	We ontwikkelen nieuwe voorzieningen t.b.v. machtigen conform de Common Ground visie maar houden er rekening mee dat ook bestaande voorzieningen machtigen moeten ondersteunen. Bijvoorbeeld door bestaande voorzieningen niet of minimaal aan te passen maar via 'encapsulation' (inkapseling) een laag van API's toe te voegen voor toegang voor externe systemen.
We gebruiken moderne technologie	We gebruiken bij machtigen moderne technologie, daarbij passende stijlen en technieken en zijn 'developer-friendly'. Bijvoorbeeld door naast het nu gebruikte SAML-protocol (ook) het OpenID Connect protocol te gaan gebruiken ('nieuw naast bestaand').
We geven de voorkeur aan open source software	We hebben een voorkeur voor gebruik van open source software bij de realisatie van componenten voor machtigen. Bijvoorbeeld bij vanuit de VNG geïnitieerde realisatie van referentie-implementaties waarvan leveranciers en gemeenten gebruik kunnen maken.
We gebruiken een gelaagd architectuurmodel	We gebruiken een vijf-lagenmodel om de voor machtigen gewenste informatiearchitectuur te beschrijven en visualiseren. Bijvoorbeeld bij het in beeld brengen van benodigde componenten en de functie daarvan (zie bijvoorbeeld het hoofdstuk 'Informatiearchitectuur').
We ontwikkelen en gebruiken NLX als gateway	We proberen gegevensuitwisseling voor machtigen zoveel mogelijk via de NLX-voorziening te laten verlopen. Bijvoorbeeld door de gegevensuitwisseling met de bevoegdheidsverklaringdienst te laten verlopen via NLX.

2.4. Conclusies

De op dit moment bestaande machtigingsvoorzieningen voldoen niet aan de binnen de maatschappij aanwezige behoeften en verwachtingen. Het stelsel van vertegenwoordiging wil door middel van overheidsbrede standaardisatie gebruik van machtigingen verbeteren. Zowel kwalitatief (bijv. eenvoudiger te gebruiken) als kwantitatief (bijv. meer gemachtigde diensten).

Gemeenten bieden, zowel voor burgers als bedrijven, nog zeer weinig diensten aan waarbij machtiging mogelijk is. Bij gemeenten is de wens aanwezig om hierin verandering te brengen en om, in lijn met Samen Organiseren, hierbij zoveel mogelijk samen op te trekken en te standaardiseren.

De huidige informatievoorziening bij gemeenten is niet voldoende geschikt om verantwoord gemachtigde diensten aan te bieden. Onder andere de daarbij vereiste logging en inzage worden nog onvoldoende ondersteund. Ontwikkelen van de gemeentelijke informatievoorziening in lijn met het GEMMA Gegevenslandschap maakt het mogelijk om hierin te gaan voorzien.

De door Common Ground beoogde manier van realiseren is geschikt om als gemeenten conform wetgeving aan te kunnen sluiten op het stelsel van vertegenwoordiging. Langs die weg kunnen basisvoorzieningen worden ontwikkeld voor het op een eenduidige manier loggen van verwerkingen. Daarbij is afstemming nodig met de binnen het gemeentelijk verwerkingsregister vastgelegde grondslag en doelbinding van verwerkingen. Hiervoor zijn al voorbereidende activiteiten ondernomen door de VNG en Common Ground beweging, maar gelet op het grote belang hiervan vanuit het programma Machtingen verdient dit extra aandacht.

3. Informatiearchitectuur

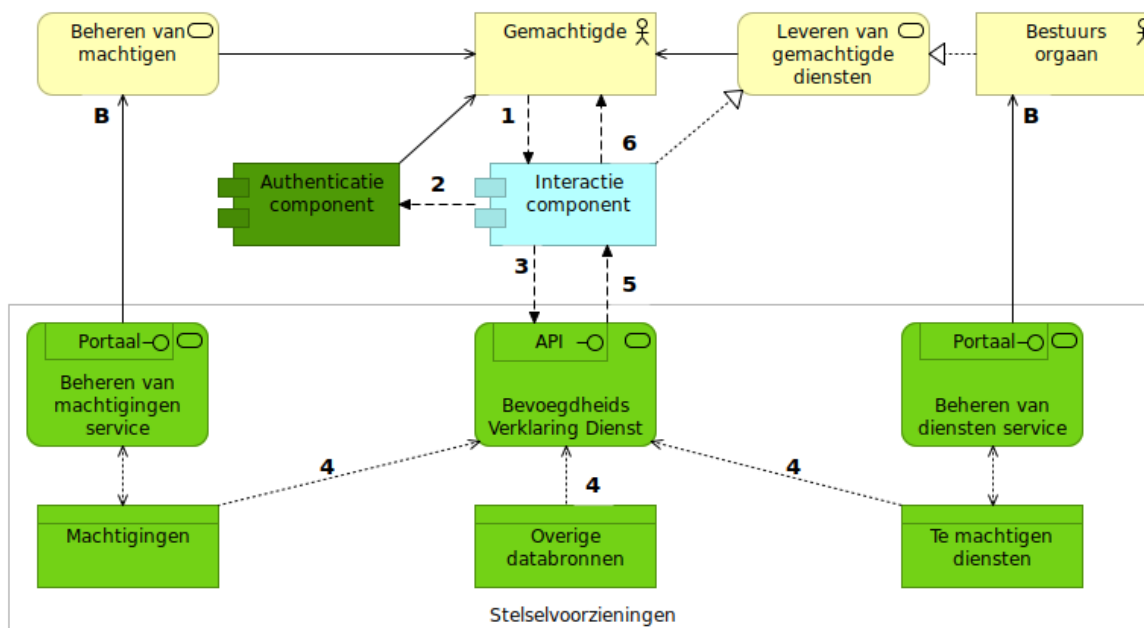
In lijn met de hiervoor geformuleerde doelen van het stelsel van vertegenwoordiging geldt dat de informatievoorziening zodanig moet zijn ingericht dat kan worden voldaan aan alle eisen en zoveel mogelijk wensen van zowel gebruikers als gemeenten zijn in te willigen. Onderstaande tabel laat zien wat de gestelde doelen zoal betekenen voor de ondersteunende informatievoorziening:

Doelen	Eisen en wensen
Volledig	Alle diensten waarbij machtigen gewenst is worden via geschikte voorzieningen ondersteund. Bijvoorbeeld door machtiging bij alle diensten binnen een dienstenset via geschikte, specifieke en generieke, componenten te ondersteunen.
Consistent	Vanuit klantperspectief gezien worden gemachtigde diensten(sets) op een vergelijkbare manier aangeboden en geleverd. Bijvoorbeeld binnen één gemeente, maar bij voorkeur ook over gemeenten heen.
Eenduidig	Gemachtigde diensten worden op eenzelfde manier aangeboden. Bijvoorbeeld door gemachtigden steeds in dezelfde volgorde authenticatie en opgeven van belanghebbende te laten doorlopen.
Gebruikers-vriendelijk:	
Betrouwbaar	Gemachtigde diensten worden zodanig aangeboden dat gebruikers inzicht kunnen krijgen in mogelijkheden en gevolgen van machtigen en inzage hebben in het gebruik van, verleende en gebruikte, machtigingen. Bijvoorbeeld via heldere toelichtende teksten en bieden van mogelijkheden om te controleren of gebruik rechtmatig heeft plaatsgevonden.
Persoonlijke benadering	Gemachtigde diensten worden zodanig aangeboden dat gebruikers het aanbod van een of meer gemachtigde diensten als 'logisch' ervaren. Bijvoorbeeld door diensten-sets te maken en aan te bieden die vanuit gebruikersperspectief logische verzamelingen van diensten omvatten.
Gemak	Gemachtigde diensten worden zodanig aangeboden dat gebruikers er snel en eenvoudig gebruik van kunnen maken. Bijvoorbeeld door bij diensten waar dit van toepassing is expliciet te vermelden dat machtiging mogelijk is en door bijvoorbeeld via een aparte webpagina te beschrijven bij welke diensten machtiging mogelijk is.
Bestuursorgaan-vriendelijk	Diensten- en machtigingenbeheer en verkrijgen van bevoegdheidsverklaringen zijn op een door gemeenten gewenste manier mogelijk. Bijvoorbeeld door gebruik te maken van eenvoudige aansluitprotocollen en standaarden die passen bij de GEMMA Gegevenslandschap-architectuur en de Common Ground wijze van realisatie.

3.1. Informatiearchitectuur landelijk

In onderstaand diagram is globaal weergegeven welke applicatiecomponenten en gegevensobjecten betrokken zijn bij gebruik van het stelsel van vertegenwoordiging. In dit diagram is alleen aangegeven wat, vanuit het stelsel gezien, een bestuursorgaan minimaal moet hebben ingericht om te kunnen communiceren met gemachtigden en de centrale stelselvoorzieningen. In de paragraaf 'Informatiearchitectuur gemeente' wordt meer in detail beschreven welke applicatiecomponenten in lijn met de GEMMA Gegevenslandschap-architectuur wenselijk zijn, wat hun functie is en hoe ze samenwerken.

Door middel van cijfers is aangegeven hoe het proces kan verlopen als een gemachtigde namens een belanghebbende een gemeentelijke dienst wil aanvragen.



Toelichting³:

	Een belanghebbende heeft via een centraal portaal een gemachtigde gemachtigd om namens hem een dienst aan te vragen ⁴ .
1	Een gemachtigde vraagt bij een interactie-component (bijv. in de vorm van een eFormulier of app) namens een belanghebbende de dienst aan.
2	De interactie-component roept een authenticatie-component aan waarmee de gemachtigde zich kan authenticeren.
3	De interactie-component vraagt aan de Bevoegdheid-Verklaring-Dienst of de gemachtigde inderdaad gemachtigd om namens een opgegeven belanghebbende de gevraagde dienst uit te voeren.
4	De Bevoegdheidsverklaringdienst raadpleegt het machtigingen- en dienstenregister en eventueel andere van toepassing zijnde registers om de benodigde verklaringen op te halen.
5	De Bevoegdheidsverklaringdienst geeft de opgehaalde verklaringen terug aan de interactie-component.

³ Afgebeelde componenten worden meer in detail beschreven in het hoofdstuk 'Informatiearchitectuur gemeente'.

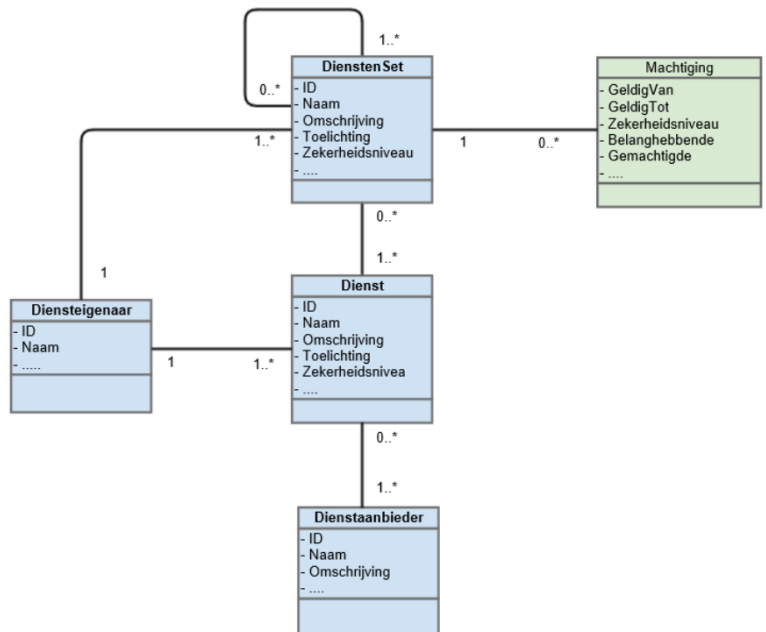
⁴ Het is in praktijk ook mogelijk dat er een machtiging is zonder dat de belanghebbende de machtiging zelf heeft verstrekt.

6	De interactie-component stelt (mede) op basis van een valide machtiging de gemachtigde in staat om namens de belanghebbende de dienst aan te vragen.
B	Zowel burgers en bedrijven als bestuursorganen krijgen via een portaal toegang tot door hen te beheren onderdelen van het stelsel van vertegenwoordiging. Burgers en bedrijven kunnen machtigingen inzien, verlenen en intrekken. Bestuursorganen kunnen kenbaar maken bij welke van door hen geleverde diensten machtiging mogelijk is. Dienst- en machtiginggegevens worden vastgelegd in centrale stelsel-registraties. Opmerking: mogelijk wordt het in een latere fase van ontwikkeling mogelijk voor stelselgebruikers om in plaats van een portaal gebruik te maken van een API voor hun beheertaken.

De aanwezigheid van een valide machtiging is niet zonder meer voldoende om een aanvrager in staat te stellen als gemachtigde op te treden. Afhankelijk van de context kan er sprake zijn van aanvullende voorwaarden waaraan voldaan moet worden.

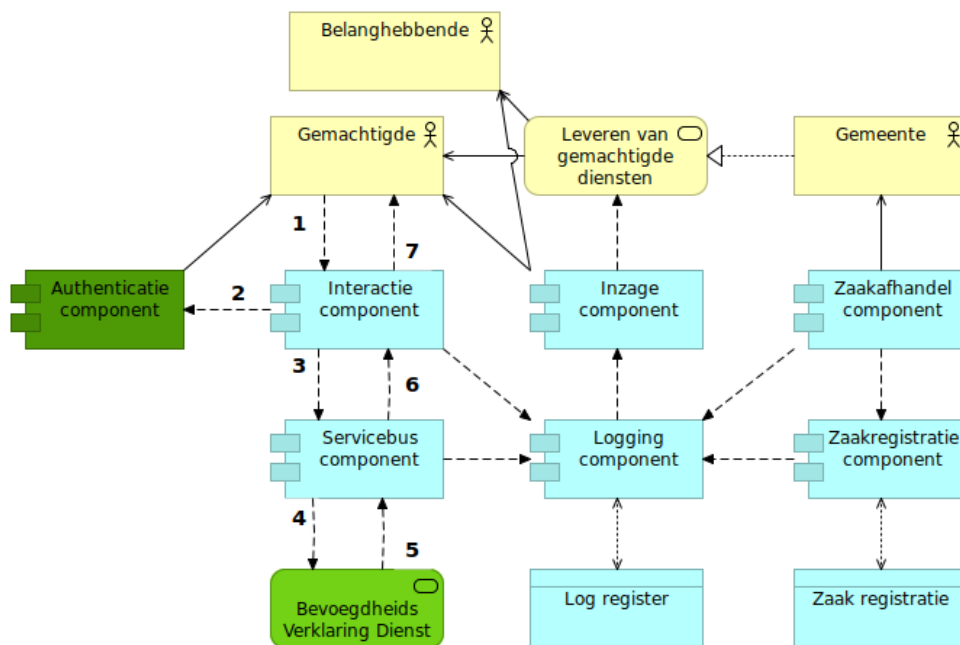
Gegevens over te machtigen diensten en machtigingen worden vastgelegd in een centrale stelselregistratie waar gebruik met te machtigen 'diensten-sets'.

In de notitie 'Handreiking bij machtigingsvoorziening' is beschreven hoe gemeenten hiermee eenduidig om kunnen gaan.



3.2. Informatiearchitectuur gemeente

In onderstaand diagram is in lijn met de GEMMA-referentiearchitectuur en het GEMMA Gegevenslandschap weergegeven welke applicatiecomponenten en gegevensobjecten (minimaal) nodig zijn om als gemeente verantwoord gebruik te maken van het stelsel van vertegenwoordiging. Door middel van cijfers is aangegeven hoe het proces verloopt wanneer een gemachtigde namens een belanghebbende een gemeentelijke dienst wil aanvragen.



Toelichting:

1	Een gebruiker vraagt binnen een interactie-component (bijv. een eFormulier of app) een gemachtigde dienst aan.
2	De interactie-component roept een externe authenticatie-component aan waarmee de gemachtigde zich kan authenticeren.
4	De interactie-component roept een servicebus-component aan om in het juiste berichtformaat de Bevoegdheid-Verklaring-Dienst te bevragen.
5	De Bevoegdheidsverklaringdienst geeft de opgehaalde bevoegdheidsverklaringen terug aan de servicebus-component.
6	De servicebus-component levert de informatie door aan de interactie-component die op basis daarvan kan concluderen of een valide machtigingsrelatie.
7	De interactie-component besluit, mede op basis van het antwoord, of de gebruiker de aanvraag mag indienen en, zo ja, start de benodigde vervolgactie (bijv. starten van een eFormulier waarmee de aanvraag gedaan kan worden).
L	Zowel de interactie-component als de servicebus-component geven metagegevens over de plaatsgevonden verwerking door aan de log-component die ze vastlegt in het (audit) log-register.
I	De inzage-component stelt gebruikers in staat om informatie op te vragen over plaatsgevonden verwerkingen waarbij zijn gegevens betrokken waren.

In aanvulling op het 'Informatiearchitectuur landelijk diagram' zijn een drietal belangrijke componenten toegevoegd die door de gemeente worden gebruikt:

- Een *servicebus-component* die binnen GEMMA wordt omschreven als een 'Component voor het routeren, transformeren en eventueel orchestreren van berichten tussen applicaties'⁵. De component fungeert als 'makelaar' tussen de interactie-component en de Bevoegdheidsverklaringsdienst. In lijn met het uitgangspunt binnen het GEMMA Gegevenslandschap "we werken met componenten" voorkomen we hiermee dat iedere interactie-component specialistische functionaliteit moet bevatten om met de Bevoegdheidsverklaringsdienst te kunnen communiceren. In de praktijk kan deze component verschillende vormen aannemen en verschillende functionaliteit bevatten. Hij kan bijvoorbeeld ook zorgen voor communicatie met een externe authenticatiedienst waardoor stap-2 in bovenstaand diagram kan vervallen. Als de component meerdere diensten gaat ondersteunen (bijv. verschillende authenticatiediensten) wordt de component ook wel 'routerings-voorziening' genoemd.
- Een *log-component* die binnen GEMMA wordt omschreven als een 'Component voor het centraal vastleggen van gegevens over de activiteiten die gebruikers uitvoeren met vertrouwelijke gegevens.'⁶ De component ontvangt metagegevens over plaatsgevonden verwerkingen van andere componenten en legt deze vast in een logging-register. In lijn met het uitgangspunt binnen het GEMMA Gegevenslandschap "'we zorgen dat informatiebeveiliging en privacy op orde zijn" en "we faciliteren regie op gegevens" is daarmee te voldoen aan het uitgangspunt dat alle verwerkingen van gegevens worden uitgevoerd conform vastgestelde doelbinding en grondslagen, en worden gelogd voor auditing en verantwoordingsdoeleinden'⁷.
- Een *inzage-component* die een gebruiker in staat stelt om informatie op te vragen over verwerkingen waarbij persoonlijke gegevens betrokken zijn. Hiermee kan langs elektronische weg worden voldaan aan het 'recht op inzage'⁸ dat gebruikers hebben conform hun AVG privacy-rechten.
- Een *zaak-afhandelcomponent* als voorbeeld van een component die gebruikt wordt door medewerkers van de gemeente bij het behandelen van de aangevraagde dienst. De component kent een eigen registratie waarin gegevens over het afhandelproces worden bijgehouden.

Opmerking: net zoals hierboven voor de servicebus-component is beschreven kunnen zich in de praktijk uiteraard situaties voordoen waarin scheiding van functionaliteit in de vorm van autonome specialistische componenten niet wenselijk of mogelijk is. Bij gebruik van SAAS-toepassingen kan communicatie met de Bevoegdheidsverklaringsdienst en het loggen van verwerkingsgegevens bijvoorbeeld onderdeel zijn van de met de leverancier overeengekomen dienstverlening.

Onderstaande paragrafen beschrijven de onderscheiden componenten en een aantal daarbij aanwezige aandachtspunten.

3.2.1. Interactie-component

Een 'interactie-component' is een component die gemachtigden via een gebruikersinterface in staat stelt om gebruik te maken van een eerder aan hen verstrekte machtiging. Een component kan bijvoorbeeld de vorm hebben van een webpagina of een mobiele app.

Afhankelijk van de context kan de interactie, of de 'klantreis', op verschillende manieren verlopen. Daarbij speelt bijvoorbeeld een rol of:

- authenticatie al eerder heeft plaatsgevonden

⁵ [GEMMA-definitie van servicebus-component](#)

⁶ [GEMMA-definitie van logging-component](#)

⁷ [GEMMA Gegevenslandschap Logging van verwerking van gegevens.](#)

⁸ [Recht op inzage conform de AVG](#)

- al bekend is welke type machtiging de gebruiker wil gebruiken
- al bekend is namens welke persoon hij als gemachtigde wil optreden
- de benodigde machtiging wel of niet aanwezig is
- er naast een aanwezige machtiging ook aan andere voorwaarden moet worden voldaan voordat een dienst wordt geleverd.

De interactie-component moet communiceren met de servicebus- en de log-component. In lijn met het GEMMA Gegevenslandschap en Common Ground kennen beide componenten daarvoor bij voorkeur een (gestandaardiseerde) RESTful-API. Of er ook communicatie met de authenticatie-component plaatsvindt hangt af van de betreffende klantreis (is de gemachtigde al ingelogd of niet) en gemaakte inrichtingskeuzes (wordt er een gemeentelijke component gebruikt of wordt het hele authenticatieproces overgelaten aan een andere voorziening zoals de Logius-routeringsvoorziening).

3.2.2. Authenticatie-component

Een 'interactie-component' verzorgt het authenticeren van een gemachtigde of belanghebbende om te bepalen of aan machtigingen gerelateerde acties (mogen) worden uitgevoerd. Op dit moment gebruiken gemeenten hiervoor vooral DigiD voor burgers en eHerkenning voor bedrijven. Conform de Europese eIDAS-verordening moeten gemeenten ook Europees erkende inlogmiddelen accepteren binnen hun digitale dienstverlening. Vooralsnog geldt voor het Stelsel van Vertegenwoordiging dat BSN of KvK-nummer bekend moet zijn om te kunnen vaststellen of er een valide machtiging aanwezig is. Op dit moment zijn dus alleen inlogmiddelen te gebruiken die in staat zijn om na authenticatie (een af te leiden) BSN of KvK-nummer te retourneren.

Naast dit type authenticatie waarbij realtime wordt bepaald of iemand met voldoende zekerheid is te authenticeren is de verwachting dat

In de (nabije) toekomst zullen ook andere vormen van authenticatie toegepast gaan worden. Conform de Wet Digitale Overheid kunnen ook private inlogmiddelen worden toegestaan. Bijv. via attriboot-gebaseerde authenticatie zoals toegepast bij de IRMA app⁹ die attributen op de smartphone van een gebruiker opslaat om daarmee met een bepaalde mate van zekerheid de identiteit van de gebruiker te kunnen overleggen.

Afhankelijk van de afspraken tussen partijen kan authenticatie ook deel uitmaken van de dienstverlening die door een externe component wordt geboden. Bijvoorbeeld via de Routeringsvoorziening¹⁰.

3.2.3. Servicebus-component

De servicebus-component verzorgt op verzoek van een interactie-component de communicatie met de Bevoegdheidsverklaringsdienst. Ook hier geldt dat er, afhankelijk van de context en gemaakte inrichtingskeuzes, verschillende patronen mogelijk zijn, die afhangen van of:

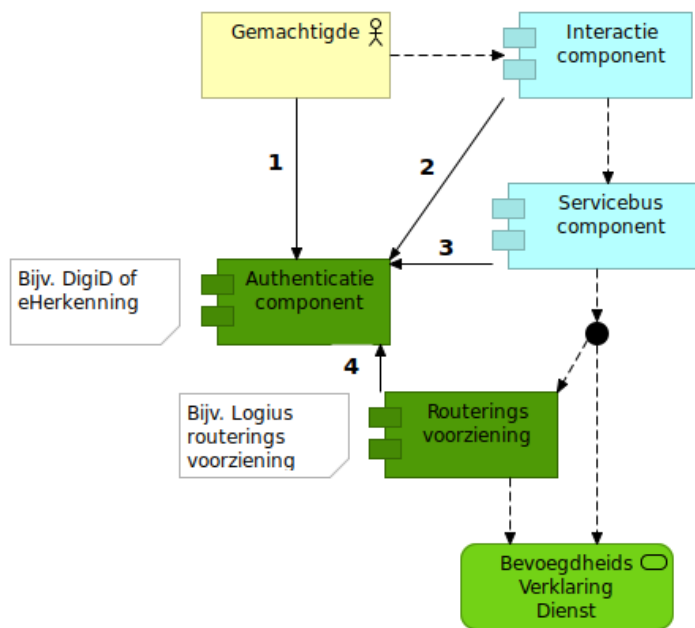
- een interactie-component zelf authenticatie initieert of
- de servicebus-component dit initieert of
- dat er gebruik wordt gemaakt van een externe voorziening die als makelaar fungeert en authenticatie met achterliggende voorzieningen verzorgt (bijv. de Logius-Routeringsvoorziening).

⁹ <https://privacybydesign.foundation/irma/>

¹⁰ De [routeringsvoorziening](#) wordt ontwikkeld door Logius met als doel om overheidsorganisaties te ontzorgen. Via één koppelvlak kunnen daarmee aan gebruikers verschillende inlogmiddelen worden aangeboden (bijv. alle tot eIDAS toegelaten middelen). Het is nog onzeker of voor het afnemen van diensten van de Bevoegdheidsverklaringsdienst van de routeringsvoorziening gebruik kan worden gemaakt en of de routeringsvoorziening precies gaat leveren.

Authenticatie moet in alle gevallen hebben plaatsgevonden voordat de Bevoegdheidsverklaringsdienst wordt aangeroepen.

Het tijdstip en de manier waarop een gebruiker zich moet authenticeren en aangeven namens wie hij handelt kan verschillen. In overleg met gemeenten wordt geprobeerd om hier in de toekomst zo eenduidig mogelijk mee om te gaan en benodigde acties zodanig te ordenen dat gebruikers hun taken eenvoudig en snel kunnen uitvoeren¹¹. Door meerdere gemeenten is al aangegeven dat het vanuit gebruikersperspectief wenselijk lijkt om de klantreis zodanig te organiseren dat vroegtijdig is aan te geven of iemand namens zichzelf of namens een belanghebbende een dienst wil aanvragen. In het diagram hieronder is weergegeven dat er op verschillende momenten authenticatie plaats kan vinden.



Toelichting van verschillende patronen:

1	Een gebruiker heeft zichzelf al eerder geauthenticeerd (bijv. om een andere dienst af te nemen).
2	De interactie-component stuurt de gebruiker door naar een authenticatiedienst.
3	De servicebus-component stuurt de gebruiker door naar een authenticatiedienst.
4	Als gebruik wordt gemaakt van de routeringsvoorziening kan die de gebruiker doorsturen naar een authenticatiedienst.

Het aangeven door een gemachtigde welke belanghebbende hij wil vertegenwoordigen kan al bij de gemeente plaatsvinden of tijdens het gebruik van de BVD. Gebeurt het bij de gemeente dan zal deze informatie worden meegegeven bij aanroep van de Bevoegdheidsverklaringsdienst. Is dit niet het geval dan moet de Bevoegdheidsverklaringsdienst het via een dialoog bij de gemachtigde uitvragen. Deze laatste werkwijze wordt toegepast in de lopende pilot binnen de zorgsector en is de voorziene werkwijze tijdens plateau-1 van het stelsel van vertegenwoordiging. Rekening houdend met de verschillende situaties en klantreizen waarin gebruik van machtigingen wenselijk is worden hopenlijk in plateau-2 beide scenario's ondersteund.

De Bevoegdheidsverklaringsdienst zal een bericht naar de servicebus-component retourneren met daarin een bevoegdheidsverklaring. Uit de bevoegdheidsverklaring is af te leiden of de gebruiker gemachtigd is om de

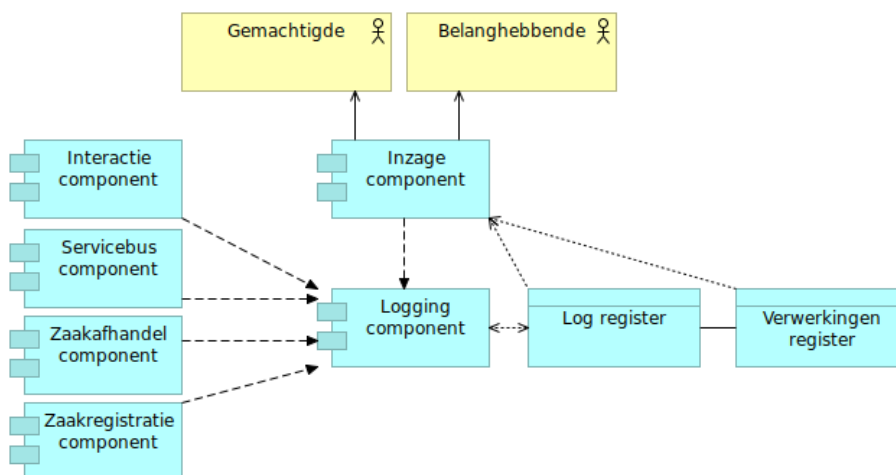
¹¹ Een voorbeeld van taakgericht vanuit gebruikersperspectief inrichten is om te zorgen dat gebruikers zich maar eenmalig hoeven te authenticeren en na het uitvoeren van een taak als gemachtigde ook andere taken waarvoor zij gemachtigd zijn kunnen uitvoeren.

aangevraagde dienst namens de belanghebbende aan te vragen. Op basis van *concept*-documentatie van de Bevoegdheidsverklaringsdienst bevat een retour-bericht globaal de volgende type gegevens:

Gegeven	Voorbeeld waarde
Soort identificatie	BSN of OIN
BSN of OIN van de vertegenwoordigde partij (belanghebbende)	123456789 of 00000004000000006000
Dienstverlener identificatie	
Dienstenset identificatie	
Dienst identificatie	
Tijdstip controle geldigheid van de machtiging	
Vervaldatum machtiging	

3.2.4. Log-component

Het gemeentelijk gegevenslandschap hanteert als uitgangspunt dat verwerkingen door informatiesystemen gerelateerd moeten zijn aan in het gemeentelijk verwerkingenregister opgenomen verwerkingen. Alle verwerkingen van gegevens moeten worden uitgevoerd conform vastgestelde doelbinding en grondslagen, en worden gelogd voor auditing en verantwoordingsdoeleinden. Dit is voorwaardelijk om compliant te kunnen zijn aan de wet- en regelgeving op het gebied van privacy en bescherming van persoonsgegevens. Al de informatie die vereist is voor het kunnen afleggen van verantwoording en het bieden van transparantie dient in een logregister opgenomen te worden.



In bovenstaand diagram is weergegeven dat van alle bij machtigingen betrokken componenten verwacht wordt dat ze metagegevens over plaatsgevonden verwerking doorgeven aan de logging-component die deze vastlegt in het log-register. Als een verwerking niet kan worden gelogd dan mag de verwerking niet worden uitgevoerd.

Logging, log-register en verwerkingenregister moeten op elkaar afgestemd zijn zodat is te verantwoorden dat plaatsgevonden verwerking stroken met de in het verwerkingen-register vastgelegde gegevens over doelbinding en grondslag. Er is nog geen vastgestelde standaard voor de wijze waarop loggegevens, logregister en verwerkingenregister moeten worden ingericht. Vooralsnog geldt het VNG-Realisatie Logging-informatiemodel¹² als uitgangspunt. Binnen Common Ground loopt een initiatief om op dit vlak tot standaardisatie te komen.

¹² <https://github.com/VNG-Realisatie/gemma-verwerkingen>

In de notitie 'GEMMA Gegevenslandschap - Logging van verwerking van gegevens' zijn verschillende inrichtingsvarianten beschreven om logginggegevens vast te leggen. Het staat gemeenten bijvoorbeeld vrij om een centraal gemeentelijk logregister in te richten, of logregisters per informatiesysteem bij te houden. Vanuit de wens om voor gespecialiseerde taken autonome componenten te gebruiken is in bovenstaand diagram uitgegaan van de situatie dat er gemeentebreed gebruik wordt gemaakt van dezelfde log-component en hetzelfde log-register.

Een aandachtspunt bij het gebruik van machtigingen is dat er altijd meerdere gebruikers (personen en/of bedrijven) bij betrokken zijn. Voor iedere gebruiker waarvan gegevens worden verwerkt moet een apart logrecord worden aangemaakt zodat gegevens apart opvraagbaar zijn.

Verder geldt voor transacties die organisatiegrenzen overschrijden, zoals bij machtigen, logrecords bij voorkeur een unieke log-identificatie kennen waarmee logrecords aan elkaar zijn te relateren. Hiervoor zal de Bevoegdheidsverklaringsdienst in staat moeten zijn om een log-identificatie te ontvangen en bij de aldaar vastgelegde loggegevens op te slaan en opvraagbaar te maken.

3.2.5. Inzage-component

Iedere gebruiker waarvan de gegevens betrokken waren bij een plaatsgevonden verwerking moet daar inzicht in kunnen krijgen. Om dit mogelijk te maken moeten bij processen waarbij een machtiging is gebruikt logrecords zijn aangemaakt in het log-register. Het log-register dient samen met het verwerkingenregister als bron voor verantwoording van het handelen van de gemeente richting burgers, bedrijven en bestuur.

De inzage-component moet zowel gemachtigde als belanghebbende in staat stellen om, na authenticatie en autorisatie, op te vragen bij welke bewerkingen hun (persoons)gegevens zijn gebruikt. Ook de bevraging van loggegevens zelf wordt gelogd. Het GEMMA Gegevenslandschap heeft als uitgangspunt dat de logregistratie via één gestandaardiseerde API wordt ontsloten waarvan, onder andere, de inzage-component gebruik kan maken. De inzage-component kan bijvoorbeeld onderdeel zijn van een gemeentelijk (bijv. MijnGemeente) of landelijk (bijv. Mijn Overheid) portaal. Opvragen of, en zo ja welk, gebruik van een machtiging heeft plaatsgevonden kan via een centrale stelselvoorziening.

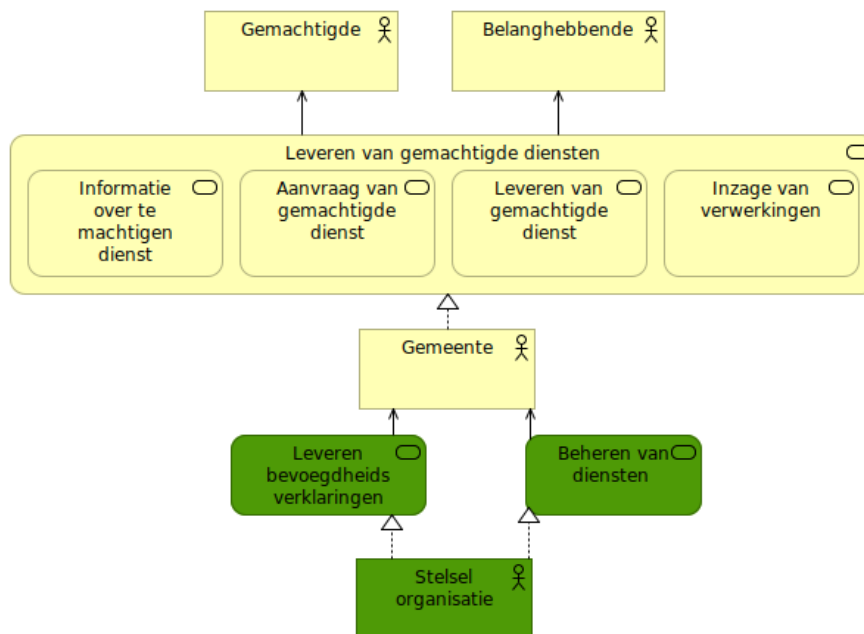
Zowel de centrale machtigingsoplossing als de gemeente moet zorgen voor logging en inzage in plaatsgevonden verwerkingen. Gebruik van unieke log-identifiers biedt de mogelijkheid maakt inzage mogelijk in de verwerking van gegevens bij verschillende betrokken partijen. Om een complete audit-trail te kunnen samenstellen zal het koppelvlak over dit type functionaliteit moeten beschikken.

Meer informatie over het het loggen van verwerkingsgegevens en het kunnen inzien daarvan is te vinden in de notitie 'GEMMA Gegevenslandschap – Logging van verwerking van gegevens'¹³.

¹³ <https://www.gemmaonline.nl/index.php/Gegevenslandschap>

3.3. Leveren van gemachtigde diensten

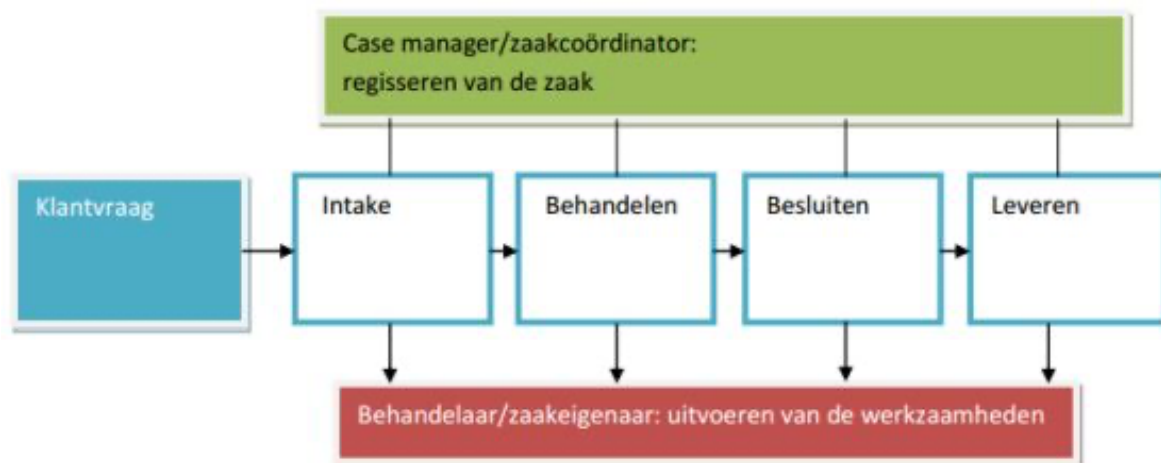
Hiervoor is beschreven welke applicaties en gegevensbronnen een rol spelen als een gebruiker gemachtigde diensten wil afnemen en als een betrokkene inzage wil in plaatsgevonden verwerkingen. Nadat is vastgesteld dat een gebruiker geautoriseerd is om als gemachtigde een dienst af te nemen moet(en) de betreffende dienst(en) uiteraard op een juiste manier geleverd gaan worden.



In bovenstaand diagram is globaal weergegeven dat het leveren van de gemachtigde dienst een van de processtappen is in het te doorlopen proces. De dienst kan zowel aan de belanghebbende als, in mindere mate, aan de gemachtigde geleverd worden. Bijvoorbeeld als voor de belanghebbende bijstand is aangevraagd maar de belanghebbende (delen van) de berichtgeving daarover moet ontvangen.

Gelet op de veelheid en diversiteit aan gemeentelijke diensten is niet eenduidig te beschrijven hoe het leveren van een gemachtigde dienst precies moet plaatsvinden. Wel zijn er een aantal algemeen geldende aandachtspunten te benoemen.

Binnen gemeenten zijn verschillende typen processen te onderscheiden. We gebruiken hieronder 'zaakgericht werken' als een veel voorkomende, procesgerichte, manier om aan te geven op welke momenten het werken met machtigen speciale aandacht vraagt. Zowel bij zaakgericht werken als het gebruik van machtigingen is een belangrijke doelstelling om burgers en bedrijven optimale dienstverlening te bieden. Met behulp van machtigen kunnen gemeenten nieuwe, of gebruikersvriendelijkere, diensten leveren. Hieronder is afgebeeld welke proces-stappen NORA onderscheidt wanneer een proces zaakgericht wordt doorlopen.



In zijn algemeenheid geldt bij gebruik van machtigen dat er bij iedere proces-stap rekening moet worden gehouden met het feit dat een dienst-aanvrager en belanghebbende niet dezelfde persoon zijn.

- Intake** Er moet rekening mee worden gehouden dat tijdens een aanvraag (vaak in de vorm van een e-formulier of andere interactiecomponent):
- zowel gegevens over de gemachtigde als de belanghebbende moeten worden verzameld en vastgelegd
 - gegevens over de plaatsgevonden authenticatie en autorisatie worden vastgelegd.
- Behandelen** Er moet rekening mee worden gehouden dat:
- tijdens de intake verzamelde gegevens, geautomatiseerd of handmatig, correct (kunnen) worden vastgelegd
 - duidelijk is voor de behandelaar welke personen, in welke rol, bij een aanvraag betrokken zijn
 - betrokkenen verschillende rechten hebben (bijv. bij het verstrekken van of bieden van inzage in gegevens)
 - betrokkenen verschillende plichten hebben (bijv. om gegevens te controleren of aanvullend te verstrekken)
 - de actualiteit van machtiging wordt gecontroleerd op momenten waarop actualiteit van machtiging van belang is (bijv. door dan opnieuw te controleren of de gebruikte machtiging nog valide is).
- Besluiten** Er moet rekening mee worden gehouden dat:
- het context-afhankelijk is of een genomen besluit bekend wordt gemaakt aan belanghebbende en/of gemachtigde.
- Leveren** Er moet rekening mee worden gehouden dat:
- het context-afhankelijk is of het betreffende product of dienst aan de belanghebbende wordt geleverd op dezelfde manier als dat de belanghebbende het product zelf had aangevraagd (bijv. omdat de gemachtigde de dienst geleverd moet krijgen of bij levering betrokken moet worden).
- Regisseren en uitvoeren** Gelet op het feit dat in gebruik zijnde applicaties (nog) niet altijd zijn toegerust op het goed ondersteunen van zaken waarbij sprake is machtiging moet bij regisseren en uitvoeren van werkzaamheden extra zorgvuldigheid worden betracht.

Gaan werken met machtigen vraagt dus zowel om aanpassingen in de manier van werken als in de daarbij gebruikte informatiesystemen. Medewerkers zullen extra zorgvuldig moeten, en mogelijk andere keuzes tijdens het behandelproces moeten maken, bij zaken waar sprake is van een machtigingsrelatie. Informatiesystemen moeten in staat zijn om, zowel in vastlegging van gegevens als in procesinrichting, rekening houden met mogelijke de machtiging. Dit kan bijvoorbeeld betekenen dat:

- afhankelijk van of er van een gemachtigde sprake is of niet, verschillende processen moeten worden ingericht (bijv. omdat de belanghebbende voor bepaalde activiteiten zelf toestemming moet geven of omdat de gemachtigde minder informatie mag krijgen dan de belanghebbende);
- afhankelijk van of er van een gemachtigde sprake is of niet, rekening moet worden gehouden met wie er via welk kanaal wat gecommuniceerd wordt. Bij de communicatie met gemachtigden en belanghebbenden kunnen zowel wettelijke voorschriften als persoonlijke voorkeuren een rol spelen. Het gaat hier zowel om notificaties, formele berichten als informele berichten.
- verwerkingsgegevens van zowel gemachtigden als belanghebbenden worden gelogd;
- tijdens behandeling optredende veranderingen met betrekking tot machtiging (bijv. intrekking van een machtiging) correct worden verwerkt (zie ook Bijlage 1 'System-to-system').

4. Technische architectuur

Zolang wordt voldaan aan de eisen die het stelsel van vertegenwoordiging stelt aan deelnemers kunnen gemeenten zelf bepalen hoe zij de daarbij gebruikte infrastructuur inrichten. Op dit moment zijn nog niet alle eisen bekend die het stelsel van vertegenwoordiging stelt aan deelname.

In algemene termen geldt dat gemeenten naar verwachting:

1. gegevens over door hen ondersteunde diensten en dienstensets moeten gaan beheren via een interactieve stelsel-voorziening;
2. via een beveiligde verbinding gegevens met de Bevoegdheidsverklaringsdienst kunnen uitwisselen;
3. over software moeten beschikken die voldoet aan de van toepassing zijnde koppelvlak-specificaties.

Ad 1) Qua techniek is een hedendaagse browser en een veilige internetverbinding hiervoor voldoende.

Ad 2) Hierin zijn verschillende varianten en combinaties mogelijk zoals het gebruik van:

- a. NLX als component die aan beide zijden van de uitwisseling voor veilige uitwisseling zorgt;
- b. GGI-Netwerk als beveiligd netwerk om de gemeente infrastructuur te verbinden met de Logius-infrastructuur;
- c. PKI-overheid certificaten om met TLS beveiligde verbindingen op te zetten.

Ad 3) De koppelvlak-specificaties zijn nog niet volledig bekend. In de lopende pilot in de zorgsector wordt gebruik gemaakt van SAML als protocol om authenticatie- en autorisatiegegevens uit te wisselen. Gelet op de wensen vanuit gemeenten om op een moderne manier bijvoorbeeld ook mobiele toepassingen te ondersteunen verdient gebruik van OpenID-Connect de voorkeur. Deze standaard is momenteel bij het Forum Standaardisatie in behandeling¹⁴.

¹⁴ <https://www.forumstandaardisatie.nl/standaard/oidc>

5. Machtigen in het vijf-lagenmodel

Eerdere hoofdstukken beschrijven welke applicaties en gegevensverzamelingen een rol spelen als een gemeente het werken met machtigingen gaat ondersteunen. Er zijn daarbij uiteraard verschillende varianten mogelijk om een en ander te realiseren.

Binnen de informatievoorziening zoals die nu bij de meeste gemeenten aanwezig is, is het zeer lastig of helemaal niet mogelijk om het gebruik van machtigingen verantwoord te ondersteunen:

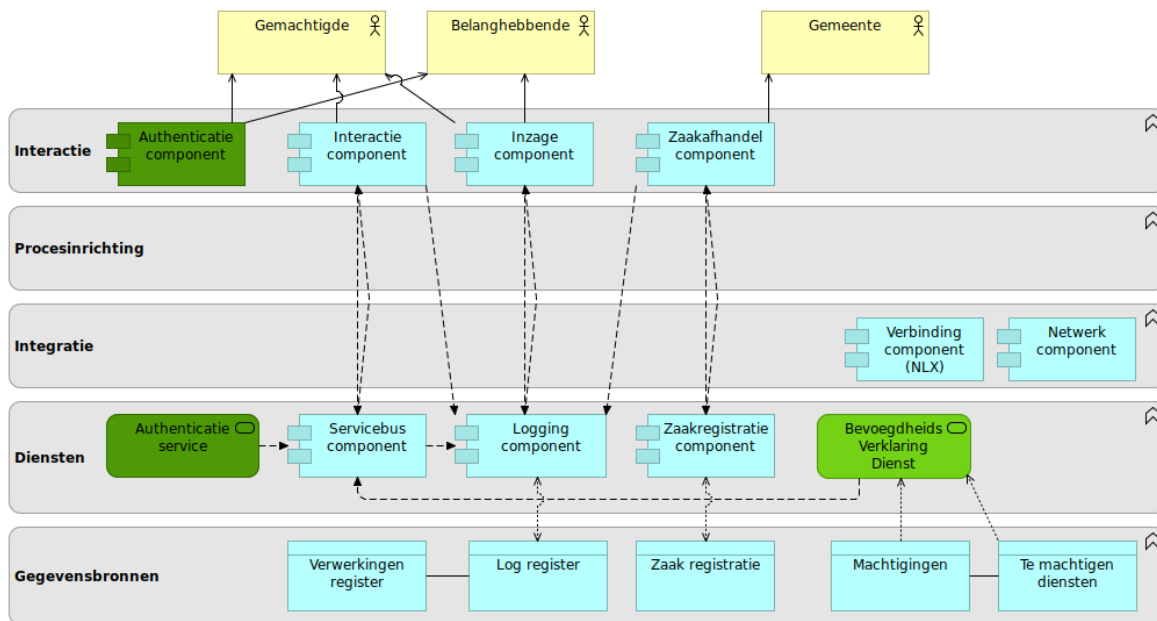
- veel applicaties en voorzieningen zijn niet ontworpen om rekening te houden met de mogelijkheid dat er gebruik van machtigen plaats kan vinden;
- er zijn geen geschikte voorzieningen aanwezig om gegevensverwerkingen te loggen;
- er zijn geen voorzieningen voor gemachtigde, belanghebbende of organisatie, om inzage te krijgen in plaatsgevonden verwerkingen.

Ontwikkeling in lijn met het GEMMA Gegevenslandschap, en conform de Common Ground aanpak, maakt het mogelijk om aan de benodigde ondersteuning te kunnen bieden. De onderstaande afbeelding toont hoe eerder onderscheiden componenten zijn te positioneren in het vijf-lagen architectuurmodel dat binnen het GEMMA Gegevenslandschap en Common Ground wordt gebruikt en waarbij iedere laag een bepaald type functionaliteit levert.

De afbeelding heeft als doel om een indruk te geven van waar bepaalde soorten functionaliteit in het vijf-lagen model worden gepositioneerd. Omwille van de 'leesbaarheid' worden met name applicatiecomponenten en gegevensbronnen afgebeeld waarbij geldt dat:

- componenten in de diensten-laag feitelijk 'diensten' leveren (maar afbeelden van componenten in lijn is met eerdere diagrammen in dit document);
- de Bevoegdheidsverklaringdienst als dienst is afgebeeld omdat het hier een externe dienst betreft (waarbij de gemeente geen inzicht heeft in daarbij gebruikte componenten)
- 'Authenticatie' is afgebeeld als front-end component voor gebruikers om zich te kunnen authenticeren én als dienst die een interactie-component informeert over de plaatsgevond authenticatie¹⁵.
- externe componenten en diensten grijs zijn.

¹⁵ Zoals eerder aangegeven is het ook mogelijk dat authenticatie niet wordt geïnitieerd door een interactie-component (waardoor het diagram er wat anders uit zou zien).



Toelichting per laag:

Interactie-laag	Hierin bevinden zich de componenten die de interactie met betrokkenen verzorgen: - De authenticatie-component zorgt voor authenticatie van gemachtigden en belanghebbenden. Een gemachtigde kan zowel een natuurlijk persoon als een bedrijf zijn. - De interactie-component ondersteunt het aanvragen van diensten door gemachtigden. - De inzage-component ondersteunt inzage door gemachtigden en belanghebbenden. - De zaakafhandel-component ondersteunt gemeentelijke medewerkers bij het afhandelen van een door een gemachtigde ingediende aanvraag (bijv. een generieke zaakafhandel-component of een taakspecifieke component). - Als de gemeente gebruik maakt van een eigen beheercomponent kan daarmee worden aangegeven bij welke dienstensets de gemeente machtiging ondersteunt¹⁶.
Procesinrichting	Het is mogelijk om de logica van componenten in de interactie-laag afzonderlijk vast te leggen en te gebruiken. In dat geval bevindt zich daarvoor een gespecialiseerde component in de procesinrichting-laag. In het diagram gaan we er van uit dat dit (nog) niet het geval is maar dat proceslogica zich in interactie-componenten bevindt.
Integratie	De componenten in deze laag zorgen voor het veilig verbinden van interactie-componenten met daarbij benodigde diensten en achterliggende gegevensbronnen. Minimaal zijn nodig: - componenten waarmee een veilige netwerkverbinding is op te zetten - componenten die het veilig uitwisselen van gegevens tussen diensten verzorgen. Bijvoorbeeld een 'API-gateway' en/of 'message-broker' of, conform de Common Ground voorkeur, NLX.
Diensten	De gemeentelijke servicebus-component verzorgt in opdracht van interactie-componenten de communicatie met de Bevoegdheidsverklaringdienst.

¹⁶ De Bevoegdheidsverklaringdienst is hier weergegeven als service die dit ondersteunt. Het is ook mogelijk dat beheer van diensten, dienstensets en machtigingen plaatsvindt via een stelselvoorziening als een portaal waarop kan ingelogd. Dit is in het diagram niet afgebeeld.

	De gemeentelijke log-component verzorgt in opdracht van andere componenten het vastleggen van log-gegevens over plaatsgevonden verwerkingen in het log-register. De zaakregistratie-component legt in opdracht van de zaakafhandel-component gegevens vast in de zaakregistratie. De componenten stellen functionaliteit beschikbaar via gestandaardiseerde API's¹⁷.
Gegevensbronnen	Binnengemeentelijk zijn aanwezig: • een log-register dat fungeert als kernregistratie van log-gegevens over plaatsgevonden verwerkingen afgestemd op de vastlegging in het verwerkingenregister; • een zakenregistratie waarin ook gegevens zijn vastgelegd zodat herkenbaar is dat er sprake is van een machtigingsrelatie. Binnen stelselvoorzieningen zijn aanwezig: • een registratie van te machtigen diensten-sets • een registratie van diensten-sets die door een gemeente worden ondersteund • een registratie van bestaande machtigingen.

Positionering in het vijf-lagenmodel maakt onder meer zichtbaar dat gebruik van de GEMMA Gegevenslandschap architectuur leidt tot eenduidig gebruik van bronregistraties en beheersbaar en efficiënt gebruik van gespecialiseerde componenten. Het maakt ook zichtbaar dat goed ondersteunen van machtigen meerdere architectuurlagen raakt en om een samenhangende aanpak vraagt. Zonder gerichte architectuurkeuzes in lijn met het GEMMA Gegevenslandschap is er, gelet op de complexiteit en het feit dat de huidige informatiehuishouding nog vaak ongeschikt is om machtigen te ondersteunen, een groot risico dat er wildgroei ontstaat en wetten worden overtreden.

¹⁷ De manier waarop API's zijn gestandaardiseerd wordt elders binnen het GEMMA Gegevenslandschap beschreven.

Bijlage 1: System-to-system en baliemachtigingen

Dienstverleners en intermediairs hebben (ook) behoefte om via system-to-system (S2S) met het stelsel van vertegenwoordiging te kunnen communiceren. Voor gemeenten is het ook van belang om burgers die naar een gemeenteloket komen te kunnen helpen door op geprotocolerde wijze een machtigingsrelatie vast te leggen.

Deze functionaliteit is niet geprioriteerd voor plateau 1 van het stelsel van vertegenwoordiging, maar zal mede op basis van de ervaringen in de pilots mogelijk in plateau 2 worden gerealiseerd.

Uit een eerste verkenning kwam naar voren dat er drie gebruiksscenario's voor S2S zijn te onderscheiden:

1. Gemachtigde organisatie (intermediair) bevraagt het machtigingsstelsel via S2S.
2. Dienstverlener bevraagt het machtigingsstelsel via S2S met de vraag of een eerder aanwezige machtiging nog steeds aanwezig is.
3. Gemachtigde wil aan de balie van een overheids- of zorgorganisatie zaken doen namens een belanghebbende¹⁸.

Met name scenario's 2 en 3 zijn voor gemeenten relevant.

Ad 2) Zoals beschreven in paragraaf 3.3 'Leveren van gemachtigde diensten' kan het nodig zijn om tijdens, of zelf na, het afhandelen van een aanvraag te controleren of een vastgestelde machtigingsrelatie nog steeds actueel is. Bijvoorbeeld of de gemachtigde die namens een belanghebbende een aanvraag indiende op een later moment nog steeds de rol van gemachtigde heeft. Gelet op het belang hiervan en de frequentie waarmee toetsing nodig kan zijn is een S2S-koppeling hiervoor noodzakelijk.

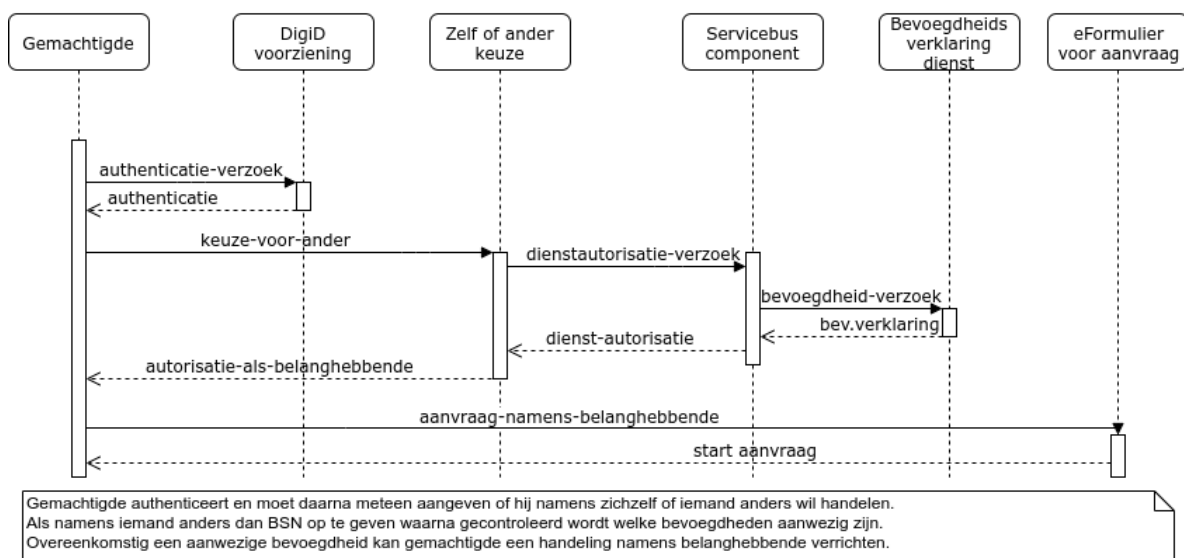
Ad 3) Gemeenten hebben als opdracht om ook langs niet-digitale weg burgers, en hun vertegenwoordigers, te ondersteunen. Bijvoorbeeld wanneer een burger die geen elektronisch authenticatiemiddel heeft snel een machtiging wil kunnen geven en daarvoor naar een gemeenteloket komt. Een baliemedewerker moet hiervoor via een geprotocolerde S2S-koppeling een beoogd belanghebbende kunnen machtigen om een burger te kunnen vertegenwoordigen.

¹⁸ In 2019 is door een groep met vertegenwoordigers uit verschillende bestuursorganen een aantal aspecten rondom 'Baliemachtigen' in kaart gebracht, zijn een aantal uitgangspunten geformuleerd en is een oplossingsrichting beschreven. Daarbij is ook geconstateerd dat er nog een aantal beleidsvragen moeten worden beantwoord. Op basis van de expertsessies wordt een Notitie oplossingsrichting Baliemachtigen opgesteld.

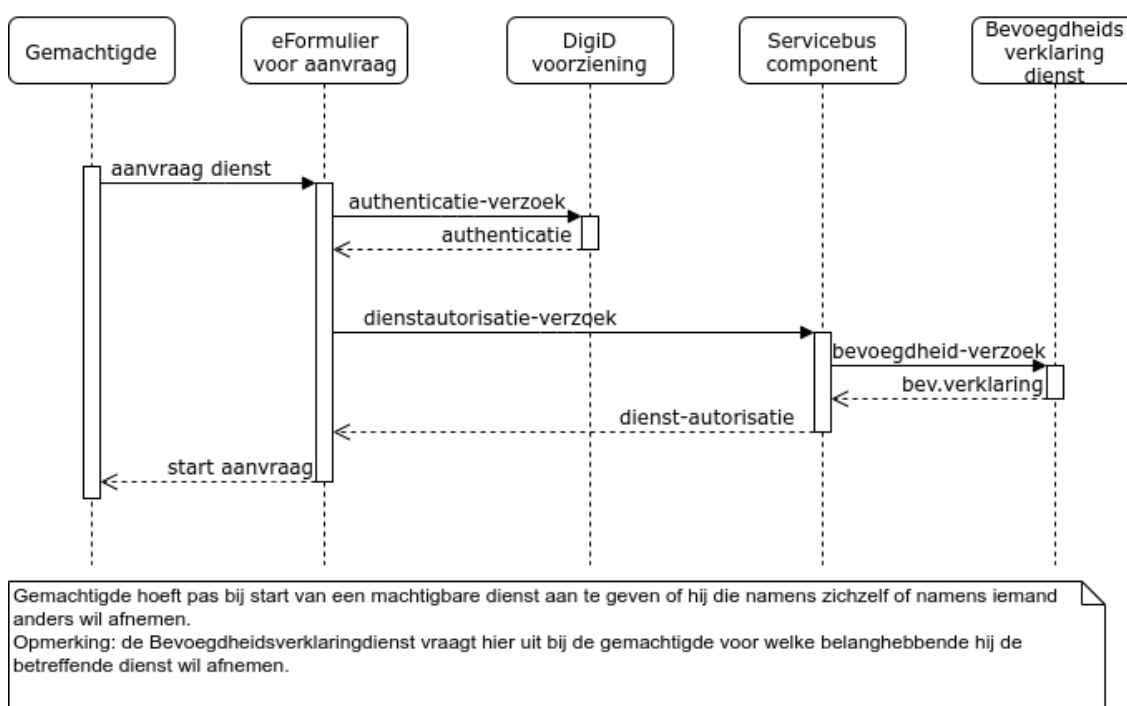
Bijlage 3: Voorbeeld use cases

Hieronder zijn enkele mogelijke use cases weergegeven via UML sequence diagrammen. Er zijn verschillende mogelijkheden om een klantreis waarbij een gemachtigde namens een belanghebbende wil handelen vorm te geven. Doelstelling is om in overleg met gemeenten te komen tot een voor dienstafnemers zo eenduidig mogelijke manier van inrichten van diensten.

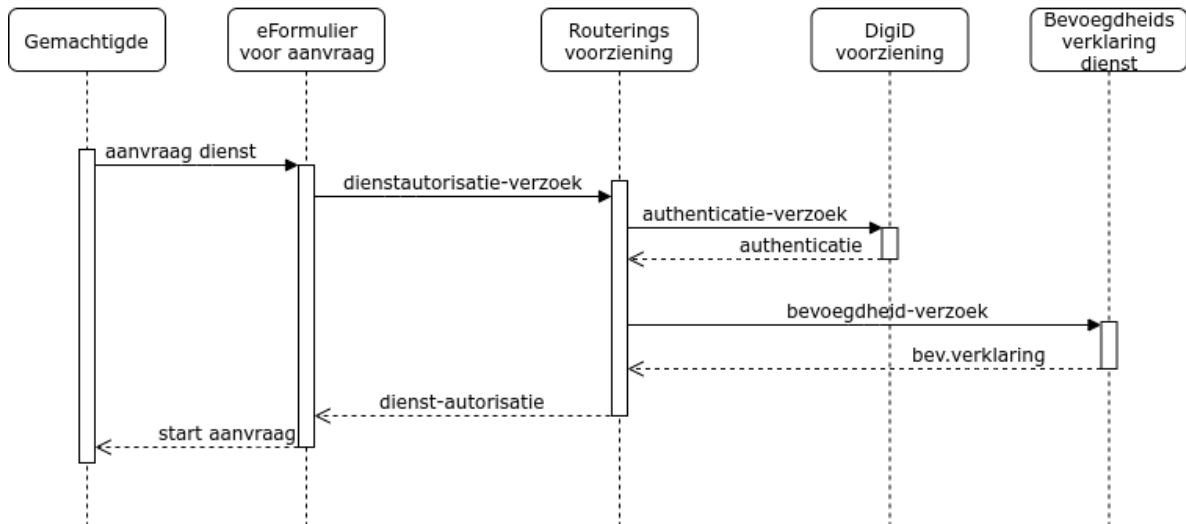
Gemachtigde na authenticatie direct vragen of hij namens zichzelf of een belanghebbende wil handelen



Gemachtigde bij aanvraag van een dienst vragen om authenticatie en machtiging



Gebruik van routeringsvoorziening voor zowel authenticatie als opvragen bevoegdheidsverklaring



Voor invulling van een eFormulier wordt gemachtigde richting routeringsvoorziening gestuurd die eerst authenticatie afhandelt en dan routeert naar de Bevoegdheidsverklaringdienst.
De routeringsvoorziening retourneert de uitkomsten naar het eFormulier.
Opmerking: voor de communicatie tussen eFormulier en Routeringsvoorziening kan ook gebruik worden gemaakt van een Servicebuscomponent in de rol van 'berichtenmakelaar'.