Logius Praktijkrichtlijn - Vastgestelde versie

Inleiding Logboek dataverwerkingen 1.0.1

Logius Praktijkrichtlijn
Vastgestelde versie 19 juni 2026

Deze versie:
https://gitdocumentatie.logius.nl/publicatie/logboek/inleiding/1.0.1/

Laatst gepubliceerde versie:
https://gitdocumentatie.logius.nl/publicatie/logboek/inleiding/

Laatste werkversie:
https://logius-standaarden.github.io/logboek-dataverwerkingen-inleiding/

Vorige versie:
https://gitdocumentatie.logius.nl/publicatie/logboek/inleiding/1.0.0/

Redacteurs:
Nil Barua (Logius)
Martin van der Plas (Logius)
Tim van der Lippe (Logius)

Auteurs:
Vedran Bilanovic (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties)
Eelco Hotting (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties)
Jeroen Mulder (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties)

Doe mee:
GitHub Logius-standaarden/logboek-dataverwerkingen-inleiding
All issues
Dien een melding in
Revisiehistorie
Pull requests

Dit document is ook beschikbaar in dit niet-normatieve formaat: PDF

Status van dit document

Dit is de definitieve versie van dit document. Wijzigingen naar aanleiding van consultaties zijn doorgevoerd.

Inhoudsopgave

§Conformiteit

Naast onderdelen die als niet-normatief gemarkeerd zijn, zijn ook alle diagrammen, voorbeelden, en noten in dit document niet-normatief. Verder is alles in dit document normatief.

Feedback en Issues

We moedigen gebruikers aan om meldingen of suggesties aan te maken via GitHub. Mocht dit niet mogelijk zijn, dan kunt u ook een e-mail sturen naar api@logius.nl.

Abstract

Dit document is onderdeel van een standaard voor het loggen van dataverwerkingen in de Nederlandse publieke sector. De governance van deze standaard wordt beschreven in het API-Standaarden beheermodel, gepubliceerd door Logius.

Context bij de standaard

De overheid wil voor burgers en bedrijven zo transparant mogelijk zijn in de omgang met hun data. Daarom is het bij de informatieverwerking in datasets belangrijk om voor elke mutatie of raadpleging vast te leggen wie deze actie wanneer uitvoert, en waarom. Voor een optimale samenwerking over organisaties en bronnen heen is voor deze logging een algemene standaard nodig.

Transparantie en verantwoording naar burgers is één van de drijfveren voor ontwikkeling van deze logging standaard, maar geen onderdeel van de standaard. De standaard richt zich op vastlegging van de logging en deze eenduidige vastlegging maakt het mogelijk om, via een extensie, inzage mogelijk te maken.

Verwijzingen

De Logboek Dataverwerkingen (LDV) standaard bestaat uit de volgende vier documenten:

Beschrijving van het document	Gepubliceerde versie	Werk versie	Repository
1. De LDV Normatieve Standaard	1.0.0	Logboek dataverwerkingen (werkversie)	logboek-dataverwerkingen

Beschrijving van het document	Gepubliceerde versie	Werk versie	Repository
2. De Algemene Inleiding	1.0.0	De Algemene Inleiding (werkversie)	logboek-dataverwerkingen-inleiding
3. Het Juridische Beleidskader	1.0.0	Juridisch Beleidskader (werkversie)	logboek-dataverwerkingen-juridisch-beleidskader
4. LDV Extensie Guideline	1.0.0	Guideline voor het schrijven van een extensie voor LDV (werkversie)	logboek-extensie-template

§1. Aanleiding en context van Logboek dataverwerkingen

Informatiehuishouding van de overheid moet op orde worden gebracht. De overheid werkt ten dienste van burgers en bedrijven. De overheid verwerkt daarvoor informatie van deze burgers en bedrijven. Het is belangrijk dat de informatiehuishouding van de overheid op orde is, zodat de overheid transparant en aanspreekbaar is, en zich daarover goed kan verantwoorden.

Dat werkt als een soort vliegwiel, omdat daardoor ook de kwaliteit van de informatie beter wordt. De overheid kan daarmee betere dienstverlening bieden en ook zorgen dat de burger minder met fouten wordt geconfronteerd, of dat overheden fouten beter en sneller kunnen herstellen als deze zich onverhoopt voordoen.

Eenduidige en integrale verantwoording over dataverwerkingen door de overheid. Belangrijk is dat overheidsorganisaties op een eenduidige manier met informatie omgaan en op een eenduidige manier informatie met elkaar uitwisselen.

Voorafgaand aan informatie-uitwisseling is het belangrijk dat transparant is waarom dat gebeurt en, achteraf moet de overheid verantwoording kunnen afleggen over de data en de wijze waarop de data is verwerkt. Zo kunnen eventuele fouten of onregelmatigheden worden hersteld en kunnen burgers hun rechten op grond van de AVG geldend maken (oa. inzage en correctie). Het gaat daarbij niet alleen om overheidsorganisaties afzonderlijk, maar het gaat er ook – juist - om dat “dé overheid” zich als geheel ten opzichte van de burger kan verantwoorden.

Een belangrijk instrument om verbetering van de informatiehuishouding te bereiken is standaardisatie. Op diverse aspecten is daarom standaardisatie nodig en worden deze ontwikkeld. Een van deze aspecten is de wijze waarop overheden zich verantwoorden. Standaardisatie daarvan vormt daarmee een puzzelstukje in het bredere geheel. Hiermee kunnen overheden hun dataverwerkingen op dezelfde wijze verantwoorden en deze verantwoording onderling relateren,

zodat de keten van dataverwerkingen tussen organisaties compleet inzichtelijk kan worden gemaakt.

§1.1 Standaard als technisch middel

De standaard Logboek Dataverwerkingen is een technische randvoorwaarde (een enabler) die organisaties in staat stelt om hun bredere doelen op het gebied van verantwoording en transparantie te bereiken. De standaard is niet het doel op zich, maar een middel om de verantwoordingsplicht van de overheid waar te kunnen maken.

Het onderscheid tussen de beleidsmatige doelen van het bredere beleidsinstrument en de technische doelen van de standaard is als volgt:

Beleidsmatige doelen (het waarom):

- Het verbeteren van de transparantie en verantwoordelijkheid van de overheid ten opzichte van burgers en bedrijven
- Het faciliteren van inzagerechten en het nakomen van wettelijke verplichtingen
- Het mogelijk maken van auditing, toezicht en kwaliteitsverbetering van de informatiehuishouding
- Het herstellen van fouten en onregelmatigheden

Deze beleidsmatige doelen worden bereikt door middel van de technische mogelijkheden die de standaard biedt. **Technische doelen** (beschreven in de normatieve standaard):

- Het bieden van interoperabele functionaliteit voor het loggen van dataverwerkingen
- Het aan elkaar relateren van logs binnen en tussen systemen
- Het specificeren van uniforme interfaces en gedrag voor logging-componenten

Deze technische doelen zijn gericht op het hoe: hoe organisaties dataverwerkingen kunnen loggen op een eenduidige en interoperabele manier.

De standaard vormt daarmee een bouwsteen binnen een groter geheel van wet- en regelgeving (zoals de AVG en AWB), organisatorische maatregelen en beleidsafspraken die samen de verantwoording van de overheid vormgeven.

§ 1.2 Scope van de Standaard Logboek dataverwerkingen

Dit beschrijft een overzicht van de scope van de standaard, inclusief de zaken die wel en niet binnen de scope van de standaard vallen.

§ 1.2.1 In scope van deze standaard

Logging over dataverwerkingen in overheidssystemen. Het uitgangspunt van deze standaard is de verantwoordingsplicht van de overheid over de uitvoering van haar taken en de wetten en kaders die daarbij horen.

§ 1.2.2 Buiten scope van deze standaard

De volgende zaken worden **niet** behandeld in deze standaard:

- **Toegangsbeheer**: Logging rondom toegang tot systemen en data, waarbij zowel succesvolle als mislukte pogingen om toegang te krijgen worden vastgelegd. Deze logs zijn bedoeld voor het controleren van wie toegang heeft tot gevoelige informatie en voor het detecteren van ongeautoriseerde toegang.
- **Toegangsverlening Logboek**: De standaard specificeert geen functionaliteit rondom het aanmaken en beheren van toegangs- en onderhoudsprofielen ten behoeve van het logboek. Voor meer informatie zie Federatieve Toegangsverlening.
- **Gebruikersactiviteiten**: Logging van namen van gebruikers die data gebruiken of verwerken.
- **Beveiligingsincidenten**: Specifieke logs voor incidenten die de beveiliging kunnen beïnvloeden, zoals malware-detectie, aanvallen of misbruik. Dit soort logging is van groot belang voor het identificeren van bedreigingen en het kunnen reageren op incidenten.
- **Technische en Systeemlogs**: Logging van systeemfouten, configuratiewijzigingen en technische problemen. Deze logs helpen bij het waarborgen van de stabiliteit en betrouwbaarheid van IT-systemen en ondersteunen het oplossen van technische problemen.
- **Logging ten behoeve van motivatie totstandkoming besluitvorming**: anders dan uitgevoerde dataverwerkingen (niet: beslisregels, algoritmes, et cetera).
- **Correcties op- en verwijdering van verwerkte data**: dit wordt gezien als verwerking en volgt de gewone route van datalogging. Voor meer informatie zie besluit 4.5.

- **Beperkingen op informatieplichten (bijvoorbeeld indien er een strafrechtelijk onderzoek plaatsvindt)**: het is aan de organisatie zelf om procedures te implementeren om beperking van inzage uit te voeren. Voor meer informatie zie besluit 4.6.

§ 1.3 Totstandkoming van de standaard

Het Logboek Dataverwerkingen is een doorontwikkeling van de conceptstandaard GEMMA Verwerkingenlogging, die door VNG Realisatie is gemaakt met als doel de naleving van AVG-verplichtingen rondom de verwerking van persoonsdata te verbeteren.

In 2023 heeft het Ministerie van Binnenlandse Zaken, in samenwerking met verschillende overheidspartijen, een project gestart om de GEMMA Verwerkingenlogging-standaard verder te ontwikkelen. Het uitgangspunt was het vergroten van de transparantie van de overheid en het verbeteren van de informatiepositie van de burger. Vanaf 2024 werd breder gekeken dan alleen de AVG; wettelijke kaders, zoals verantwoordingsverplichtingen, werden als uitgangspunt genomen voor het vormgeven van de standaard. Om aan deze eisen te voldoen, is de standaard aangepast en hernoemd tot Logboek Dataverwerkingen.

§ 1.3.1 Interdisciplinaire aanpak

Voor de ontwikkeling van de standaard Logboek Dataverwerkingen was het essentieel dat de verschillende aspecten (juridische beleidskaders, techniek, inhoud en beheer) goed op elkaar werden afgestemd. Daartoe werkte het project met een interdisciplinair team: juristen, beleidsmakers en adviseurs van BZK werkten nauw samen met technische experts van Digilab en medewerkers van Logius, de beoogde beheerder. Deze interdisciplinaire aanpak zorgde ervoor dat de standaard aansluit op juridische randvoorwaarden, eenvoudig te beheren en te implementeren is, én effectief functioneert in de praktijk. Dit laatste aspect werd getest in Digilab, waar de standaard in verschillende simulatieomgevingen (Fieldlabs) werd ingebouwd en beproefd op praktische toepasbaarheid.

§ 1.3.2 Beheer en doorontwikkeling

Om de overgang tussen ontwikkeling en beheer soepel te laten verlopen, was Logius vanaf een vroeg stadium betrokken bij het project. De inzet van Logius is in de loop van de tijd uitgebreid, zodat in 2025 het beheer van de standaard volledig kan worden overgedragen. Dit beheer wordt ingericht volgens de BOMOS-methodologie (Beheer- en OntwikkelModel voor Open

Standaarden). Het opzetten van een goede governance-structuur is een integraal onderdeel van het beheer. Hierbij zullen, naast de gebruikers van de standaard, belangrijke rollen zijn weggelegd voor MIDO (Meerjarenprogramma Infrastructuur Digitale Overheid) en het Forum Standaardisatie. Deze gremia zullen naar verwachting respectievelijk de standaard vaststellen en deze opnemen op de Pas-Toe-Of-Leg-Uit-lijst. Het Ministerie van Binnenlandse Zaken blijft opdrachtgever voor het beheer van de standaard.

§1.4 Relaties met andere standaarden

Logboek Dataverwerkingen verhoudt zich goed tot andere standaarden. Zo kan het samen werken met twee andere standaarden uit het Federatief Datastelsel. In het Federatief Datastelsel zijn 3 logstandaarden ontwikkeld, elk met een eigen toepassingsgebied en ze sluiten op elkaar aan.

- De FSC log, die bijhoudt welke transacties er zijn gedaan. Dit is op de onderste laag, het transport. Er staat in wie met wie uitgewisseld heeft en welke contracten daarbij horen.
- Het logboek toegangsbeslissingen. Daarin staat welke toegang verleend is, aan wie, waarvoor en op basis van welke regels. Doel is interne audit, het achteraf kunnen uitleggen waarom een beslissing op dat moment juist was (of misschien juist niet).
- Ons Logboek Dataverwerkingen die is voor verantwoording toe. Daarin staan verwerkingen, in de AVG-definitie, er gedaan zijn door wie en waarom.

De drie logs van de standaarden zijn verbonden door een W3C trace, zodat een totaalplaatje mogelijk is wat volledige transparantie bevordert tussen verschillende organisaties in een ketenoverzicht.

§2. Architectuur

De standaard Logboek dataverwerkingen levert geen kant-en-klare softwareoplossing. Wel biedt de standaard richtlijnen waar het Logboek dataverwerkingen van een applicatie aan moet voldoen. Dit document geeft aan hoe de standaard zich verhoudt tot de Architectuur Digitale Overheid 2030 en de *Domeinarchitectuur Gegevensuitwisseling*

§2.1 Bedrijfsarchitectuur

- *Diensten en producten*

    - De standaard Logboek dataverwerkingen is als product voornamelijk gericht op het verantwoorden van dataverwerkingen door overheden in het kader van hun taken (**Regie op Gegevens** en de **Transparante Overheid)**. Dit betekent dat het gebruik van deze standaard door overheidsorganisaties de informatiepositie van burgers en bedrijven ten opzichte van de overheid sterk verbetert zodat zij meer grip op en inzicht in hun persoonsgebonden data hebben (**inzicht in data over jezelf**). Daarnaast draagt deze standaard aan bij **Verantwoord datagebruik en ruimer meervoudig gebruik data**. Implementatie van deze standaard draagt bij aan de verantwoording over, en het doelmatig gebruik van data.

- *Kanalen*
    - Het Logboek dataverwerkingen is een service behorend bij een applicatie die specifieke data verwerkt waarover uiteindelijk verantwoording moet kunnen worden afgelegd (bijvoorbeeld persoonsdata of data over geografische objecten). De standaard geeft geen richtlijnen ten aanzien de ontsluiting van deze logdata richting belanghebbenden, wel geeft het een richting ten aanzien van de inrichting en het gedrag van het Logboek dataverwerkingen.
- *Organisatie*
    - De Overheid bestaat uit vele (semi)autonome organisaties. Door gezamenlijke afspraken te maken ten aanzien van logging van verwerkte data, ondersteunt de standaard het doel om naar de burger toe als één organisatie te kunnen verantwoorden.
- *Processen*
    - Voor het verwerken van data zijn vaak ook data nodig van andere (overheids)organisaties. De implementatie van de standaard Logboek dataverwerkingen zorgt er voor dat loggings tracing-metadata bevat zodat altijd kan worden nagegaan wat de bron van specifieke data was. De standaard ondersteunt hiermee het uitgangspunt dat (overheids)organisaties zorgen voor onderlinge samenhang van data.
- *Bedrijfsfuncties*
    - Overheidsfuncties moeten eenduidig een helder belegd zijn, het moet helder zijn welke (overheids)organisaties verantwoordelijk zijn voor het leveren van product of dienst. Door het gebruiken van de standaard Logboek datalogverwerkingen door alle dataverwerkende (overheids)organisaties op een soortgelijke manier wordt het duidelijk welke data gebruikt zijn en door wie.

§2.2 Informatiearchitectuur

- *Api's / Services*

    - Naast richtlijnen voor de inrichting en het gedrag van het Logboek dataverwerkingen, biedt deze standaard ook een aantal voorbeeld API's:
    - **Inzicht API:** deze service geeft de mogelijkheid een query uit te voeren op loggings van dataverwerkingen (nog niet beschikbaar).
    - **Register van de Verwerkingsactiviteiten:** deze service geeft de mogelijkheid de data van een Register van Verwerkingsactiviteiten te bekijken (nog niet beschikbaar).

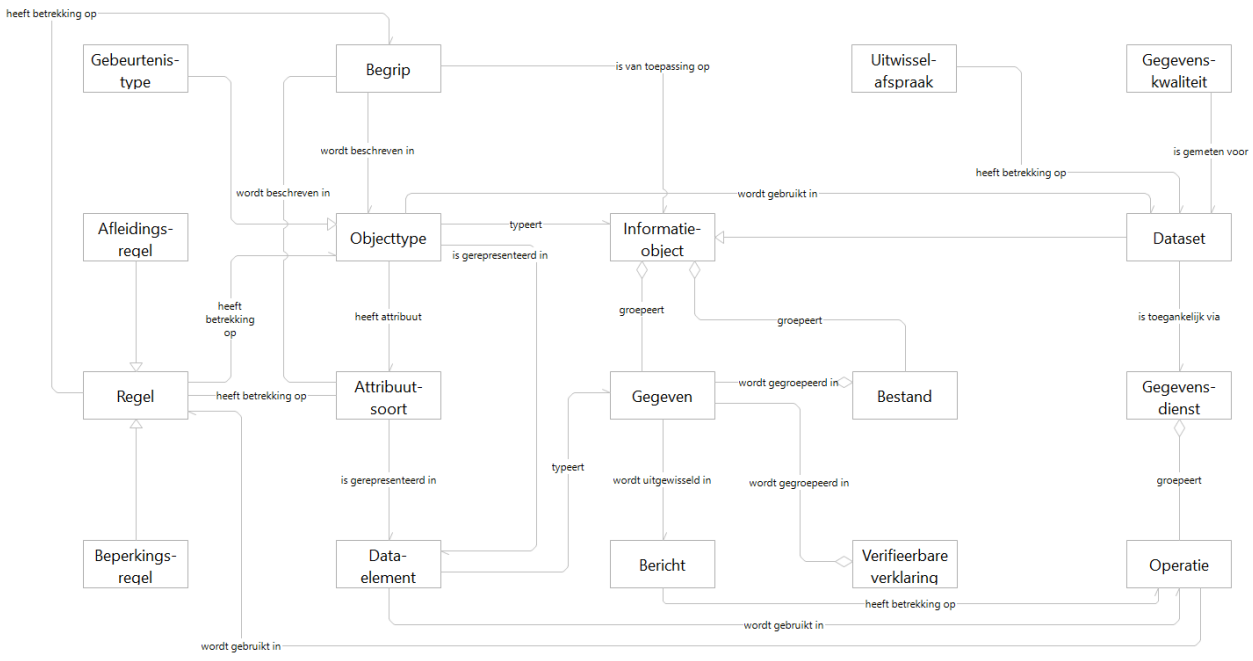
> De API's zijn ontworpen en ontwikkeld volgens de standaard Rest-API Design Rules.

- *Applicaties*
    - De standaard biedt geen applicatie aan, wel biedt het richtlijnen ten aanzien van het gedrag en invulling van het Logboek dataverwerkingen. Hiermee geeft de standaard de vrijheid aan organisaties om zelf op basis van de specifieke implementatie van een dataverwerkende Applicatie een Logboek te ontwikkelen wat qua gedrag en (meta)data gelijkvormig is over alle (overheids)organisaties heen.
- *Berichtenverkeer / datauitwisseling*
    - Het berichten verkeer met betrekking tot het Logboek dataverwerkingen heeft geen directe connectie met de burger. Wel is het van belang bij opvraag van data bij andere organisaties traceringsdata worden verstuurd en opgeslagen in het Logboek zodat altijd duidelijk wat de bron is van data die verwerkt zijn. Deze standaard biedt een traceringsmethodiek aan zodat de datauitwisseling tussen organisaties *vastgelegd en verantwoord* kan worden.
- *Data*
    - De Nederlandse Basisregistraties vervullen een essentiële rol in het vastleggen en gecontroleerd beheren van data. Organisaties kunnen aan elkaar data ter beschikking te stellen vanuit 'kernregistraties'. De standaard Logboek dataverwerkingen biedt een richtlijn voor het loggen van verwerkte data van al deze basisregistraties.

Onderstaande stelselplaat geeft een globaal overzicht van de bronhouders, de aanbieders en afnemers van data.

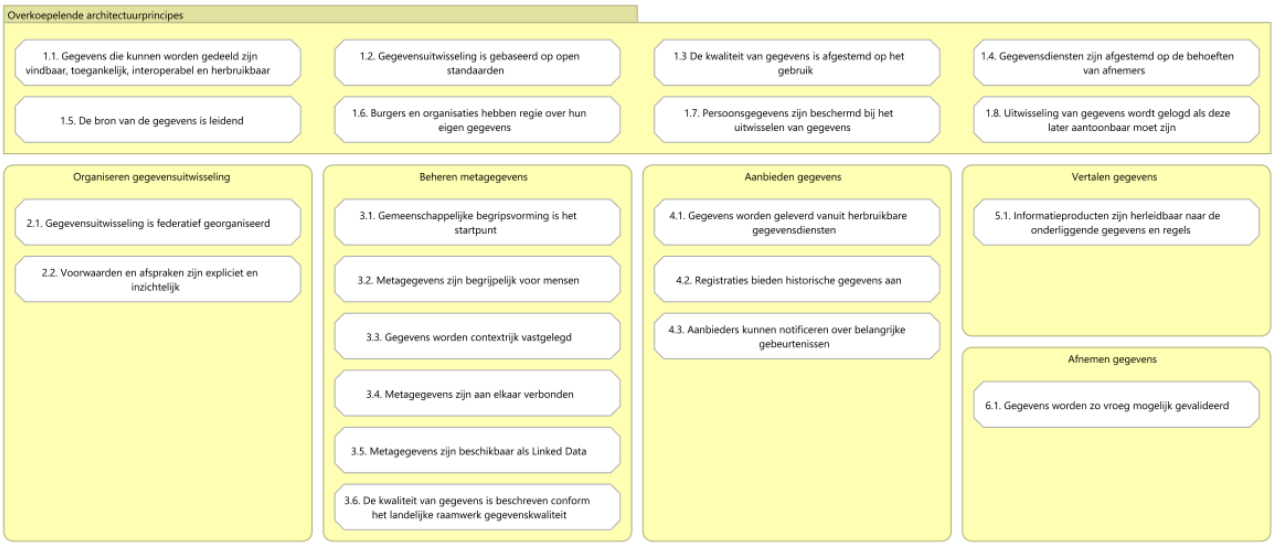
Figuur 1 Architectuur Digitale Overheid 2030

Een belangrijk kader voor de standaard Logboek dataverwerkingen is de uitwerking van het GDI meerjarenvisie op basis van de Architectuur Digitale Overheid 2030 met als specifiek onderwerp Gegevensuitwisseling. De standaard Logboek dataverwerking kan gepositioneerd worden in de GDI Gegevensuitwisseling als standaard waarin een 'Uitwisselingsafspraak' geformaliseerd wordt. Waarbij de daadwerkelijke logging betrekking heeft op de 'Operatie' in de modelplaat GDI-Gegevensuitwisseling.



Figuur 2 GDI-Gegevensuitwisseling

Onderstaand figuur geeft een overzicht van de architectuurprincipes uit het GDI meerjarenvisie en hun relatie met de belangrijkste functie voor data uitwisseling.

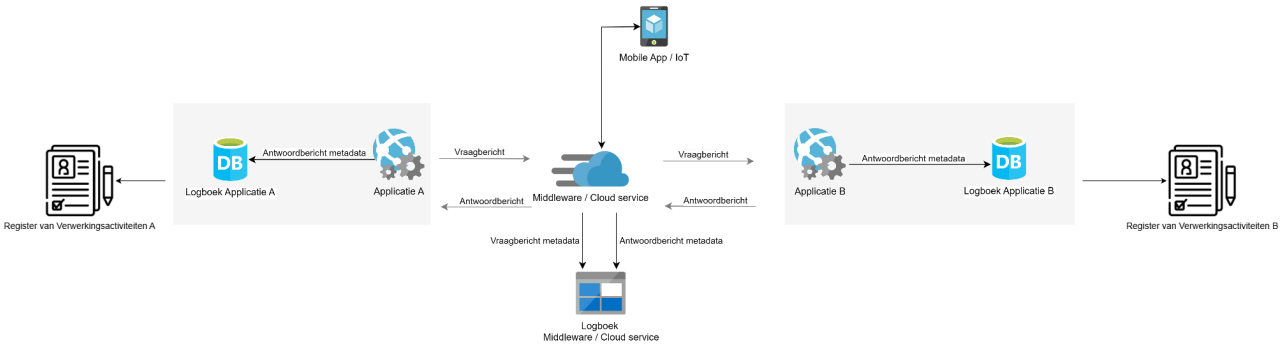


Figuur 3 MIDO/GDI Domeinarchitectuur Gegevensuitwisseling

De relatie en invulling van de standaard Logboek dataverwerkingen staat uitgewerkt in de volgende paragraaf.

§2.3 Technische architectuur

De standaard Logboek dataverwerkingen kan ook worden toegepast in een middleware- of cloud-omgeving. Het netwerkcomponent logt binnenkomende en uitgaande berichten.



Figuur 4 Technische Architectuur

Ook voor mobiele Apps en IoT (Internet of Things) geldt dat het netwerkcomponent de databerichten logt.

2.4 Software architectuur

Hoofdstuk 2.2 Componenten geeft een globaal overzicht van de benodigde softwarecomponenten om de standaard te implementeren.

2.4.1 Platformen voor dagelijkse exploitatie en huisvesting

De standaard Logboek dataverwerkingen gaat er vanuit dat de het Logboekcomponent op een beveiligd platform in een beveiligd datacenter is geïnstalleerd.

2.4.2 Aspectgebieden

- *Informatiebeveiliging*
  - De standaard Logboek dataverwerkingen gaat er vanuit dat zowel het Logboekcomponent als de data in het Logboek beveiligd zijn volgens de BIO (=Baseline Informatiebeveiliging Overheid) – zie ook Beleidskader.
- *Beheer en exploitatie*
  - Logius verzorgt het beheer en onderhoud van deze standaard volgens het BOMOS-model.

2.5 Relaties GDI architectuurprincipes en de standaard

Architectuurprincipe	Relatie met de standaard
1.1. Data die kunnen worden gedeeld zijn vindbaar, toegankelijk, interoperabel en herbruikbaar	- Logregels zijn voorzien van metadata ten aanzien van tracering zodat gerelateerde Logregels altijd gevonden kunnen worden. - Identificatoren worden aangemaakt zodat deze over de gehele wereld uniek zijn. - Het `processing_activity_id` is gerelateerd aan het Register van Verwerkingsactiviteiten zodat per Logregel altijd verwezen kan worden naar een activiteit van een (overheids)organisatie en daarmee de context direct duidelijk wordt.

Architectuurprincipe	Relatie met de standaard
1.2. Datauitwisseling is gebaseerd op open standaarden	- API's gerelateerd aan deze standaard moeten worden ontworpen en gebouwd volgens de standaarden REST-API Design Rules, OpenAPI en DigiKoppeling. - Het metadatamodel van deze standaard is gebaseerd op OpenTelemetry. Dit is een internationale standaard voor het genereren, verzamelen en exporteren van telemetrie data (metrieken, logging en tracering).
1.3 De kwaliteit van data is afgestemd op het gebruik	- Door de registratie van verwerkte data in een Logboek kan er op een later moment inzicht gegeven worden aan andere (overheids)organisaties en burgers. Eventuele foutieve data komen dan direct aan het licht en kunnen hersteld worden.
1.4. Datadiensten zijn afgestemd op de behoeften van afnemers	- Data die gelogd worden bij een dataverwerking zijn afgestemd op het doel waarvoor er gelogd moet worden (bijvoorbeeld de data die gevraagd worden op basis van de AVG-wetgeving). Er wordt niet minder opgeslagen, meer zeker niet meer dan nodig is. - Het ontwerp van het datamodel van deze standaard is gebaseerd op OpenTelemetry, vertaling van data is dus niet nodig.
1.5. De bron van de data is leidend	- Overheidsapplicaties moeten rekening houden met de onderhoud van data bij de bron. Dit betekent dat data niet zonder meer gekopieerd opgeslagen mogen worden. Bij sommige dataverwerkingen zijn data nodig van andere databronnen (in de eigen organisatie of bij een andere organisatie). De standaard Logboek Dataverwerkingen schrijft een traceringsmechanisme voor zodat kopiëren van specifieke data naar het Logboek niet nodig is, er kan altijd nagegaan worden waar data vandaan kwamen en welke data er gebruikt werden. - De standaard verwijst zo veel mogelijk naar bestaande databronnen elders in plaats van de data te dupliceren (zie besluit 4.2 en 4.4)
1.6. Burgers en organisaties hebben regie over hun eigen data	- Burgers, (overheids)organisaties en parlement hebben recht om inzicht te krijgen in verwerkte data. Door toepassing van deze standaard kan er een rapportage gemaakt worden die voldoet aan die informatiebehoefte. - De standaard Logboek dataverwerkingen biedt geen handreiking ten aanzien van de manier waarop datainzicht plaats moet vinden richting belanghebbende, wel op de in de inhoud van het datainzicht.
1.7. Persoonsdata zijn beschermd bij het	- Deze standaard gaat er vanuit dat autorisatie- en beveiligingsmechanismen worden toegepast rondom Applicatie en

Architectuurprincipe	Relatie met de standaard
uitwisselen van data	Logboek, daarom zijn er geen extra richtlijnen op dit vlak. Zie ook Beleidskader.
1.8. Uitwisseling van data wordt gelogd als deze later aantoonbaar moet zijn	- Logging van verwerkte data is de kern van deze standaard. Door gebruikt te maken van een traceringsmechanisme en unieke identificatoren, kan er altijd worden voldaan aan de eis dat ontvangen en verzonden data aan elkaar gerelateerd kunnen worden.
2.1. Datauitwisseling is federatief georganiseerd	- Logboek Dataverwerkingen maakt het mogelijk om in een gefedereerde omgeving en in informatieketens verantwoording te kunnen afleggen over datauitwisseling. Hiervoor wordt tracing ingezet, een concept dat gebaseerd op de open standaard OpenTelemetry. Zie voor enkele juridische en beleidsmatige uitgangspunten het Juridisch Beleidskader hoofdstuk 6 en hoofdstuk 8. - Nadere invulling t.a.v. datauitwisseling in het kader van inzage zal volgen als de extensie voor inzage wordt gemaakt.
2.2. Voorwaarden en afspraken zijn expliciet en inzichtelijk	- Afspraken in het kader van deze standaard zullen vooral gemaakt worden op het gebied van tracering van data binnen organisaties en over organisaties heen.
3.1. Gemeenschappelijke begripsvorming is het startpunt	- De data die gebruikt worden in deze standaard, staan vermeld en uitgelegd in het Canoniek datamodel. Het is van belang dat alle (overheids)organisatie die gebruik maken van de standaard hetzelfde beeld hebben ten aanzien specifieke data en uitwisseling daarvan om foutsituaties en verwarring te voorkomen.
3.2. Metadata zijn begrijpelijk voor mensen	- De metadata zijn veelal ontstaan op basis van de internationale standaard OpenTelemetry. Daarnaast worden de begrippen ook uitgelegd in het Canoniek Datamodel.
3.3. Data worden contextrijk vastgelegd	- Het gebruik van metadata in deze standaard is essentieel. De context wordt uitgelegd in het Canoniek Datamodel.
3.4. Metadata zijn aan elkaar verbonden	- Metadata tussen de verschillende Logboeken zijn aan elkaar gerelateerd middels de beschrijvingen en afspraken zoals gespecifieerd in de standaard .
3.5. Metadata zijn beschikbaar als Linked Data	- De gedefinieerde metadata is gerelateerd aan de standaard NL-SBB – standaard voor het beschrijven van begrippen.
4.1. Data worden geleverd vanuit herbruikbare datadiensten	- Nadere invulling volgt bij het ontwerp van de Inzage extensie.

Architectuurprincipe	Relatie met de standaard
4.2. Registraties bieden historische data aan	- Data in het Logboek mogen niet fysiek worden verwijderd; als ze niet meer geldig zijn dan wordt alleen vastgelegd dat ze niet meer geldig zijn (tenzij ze om juridische redenen vernietigd moeten worden). - De historische integriteit van Logboekdata is geborgd; oude data mogen niet worden niet overschreven. - Nieuwe formele overheidsregistraties die worden ontwikkeld, moeten de formele historie van datawerking vastleggen conform de standaard Logboek dataverwerking. Ook de wijzigingen in Register van Verwerkingsactiviteiten worden toevoegd als nieuwe verwerkingsactiviteiten met een eigen unieke identificator. Bestaande verwerkingsactiviteiten mogen niet wijzigen of verwijderd worden. Hierdoor blijven de oude verwijzingen uit de Logboek Dataverwerking intact.
4.3. Aanbieders kunnen notificeren over belangrijke gebeurtenissen	- N.v.t. Standaard beschrijft geen notificatiemechanisme voor wijzigingen in de Log.
5.1. Informatieproducten zijn herleidbaar naar de onderliggende data en regels	- Door gebruikt te maken van een traceringsmechanisme en unieke identificatoren, kan er altijd worden voldaan aan de eis dat ontvangen en verzonden data aan elkaar gerelateerd kunnen worden. De bron, en daarmee de kwaliteit en betrouwbaarheid van verwerkte data, kunnen snel en eenvoudig worden opgehaald. - Wordt eventueel nader ingevuld bij de ontwikkeling van een Inzage extensie.
6.1. Data worden zo vroeg mogelijk gevalideerd	- Validatie van logdata is een taak van de Applicatie zelf, deze standaard geeft hiervoor geen handreiking.

§3. De relatie tussen logboekelementen, waarom eigenlijk?

Logging van dataverwerkingen kunnen vaak en veelvuldig plaatsvinden. Het geheel kan groot en complex worden want sommige Logregels zijn aan elkaar gerelateerd. Deze relaties kunnen gelegd worden met Logregels met andere applicaties binnen dezelfde organisatie of met logregels van applicaties van andere organisaties.

Maar ook zijn er relaties nodig met activiteiten in het Register van Verwerkingsactiviteiten. Wat nu als alle Logregels zonder relaties worden opgeslagen? Bij een rapportage (bijvoorbeeld een verzoek tot inzage van een burger) moet nu handmatig worden uitgezocht welke dataverwerkingen

bij elkaar horen en er moet, in het ernstigste geval, ook contact worden gezocht moet andere organisaties om te onderzoeken of daar ook de nodige dataverwerkingen zijn uitgevoerd. Als er bij elke Logregel de nodige relatiedata worden bijgevoegd, kan de rapportage snel en accuraat worden gegenereerd.

3.1 Welke relatiedata moeten er dan worden opgeslagen per Logregel?

Om er zeker van te zijn dat de relatie tussen Logregels gelegd kan worden, moeten de volgende data worden geregistreerd per Logregel:

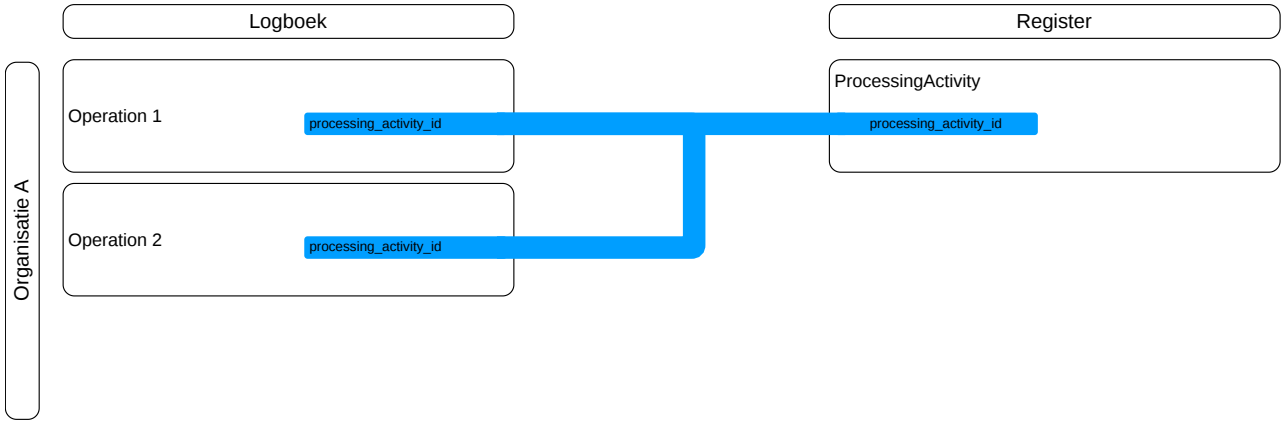
- `processing_activity_id`: elke dataverwerking die een organisatie doet, moet bekend zijn in het Register van Verwerkingsactiviteiten. Het processingActivity legt de relatie tussen de dataverwerking door een applicatie, en de activiteit gedefinieerd in het Register. Relatie tot NORA: Proces
- `trace_id`: alle logregels die voor een specifieke dataverwerking bij elkaar horen, krijgen een `trace_id`. De `trace_id`-waarde voor alle Logregels die bij elkaar horen is hetzelfde. Relatie tot NORA: Ketenproces
- `span_id`: elke individuele Logregel (Operation) krijgt een eigen, unieke `span_id` (net zoals elk databaserecord dat ook krijgt). Relatie tot NORA: Processtap

In werkelijkheid worden alle relaties door de Applicatie in een fractie van een seconde (in parallel) gelegd. Om het grote geheel beter te begrijpen, worden alle relaties hieronder stap voor stap uitgelegd.

3.2 Het logboek en het Register van Verwerkingsactiviteiten

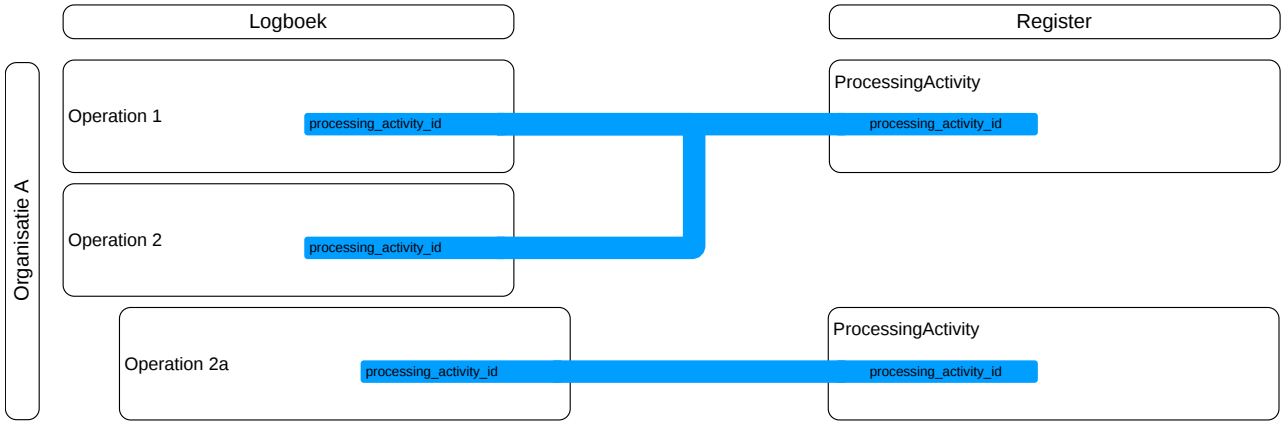
Als er een Dataverwerking plaatsvindt, moet dit altijd een relatie hebben met het Register van Verwerkingsactiviteiten. In dit Register staat informatie over de data die een organisatie verwerkt. Het Register is verplicht, een geautomatiseerde koppeling met het Logboek niet.

Bij elke Dataverwerking wordt door het Logboek een relatie gelegd met het Register door middel van het `processing_activity_id`. Als er meerdere dezelfde Dataverwerkingen ('Operations') zijn, krijgen deze dus allemaal dezelfde `processing_activity_id`.



Figuur 5 Afbeelding relaties processing_activity_id

In het geval er een Dataverwerking plaatsvindt ter ondersteuning van een andere Dataverwerking (suboperation), dan kan deze ondersteunende Dataverwerking een eigen `processing_activity_id` krijgen. Deze kan anders zijn dan het `processing_activity_id` van de 'hoofdprocessingActivity'.



Figuur 6 Afbeelding relaties processing_activity_id tussen Logboek en Register

Bij een Dataverwerking kan het zijn dat data moeten worden opgevraagd bij een andere organisatie. Deze organisatie heeft zelf ook een Register van Verwerkingsactiviteiten. In dit Register staat beschreven dat een specifieke organisatie specifieke gegevens mag opvragen als aparte operation.

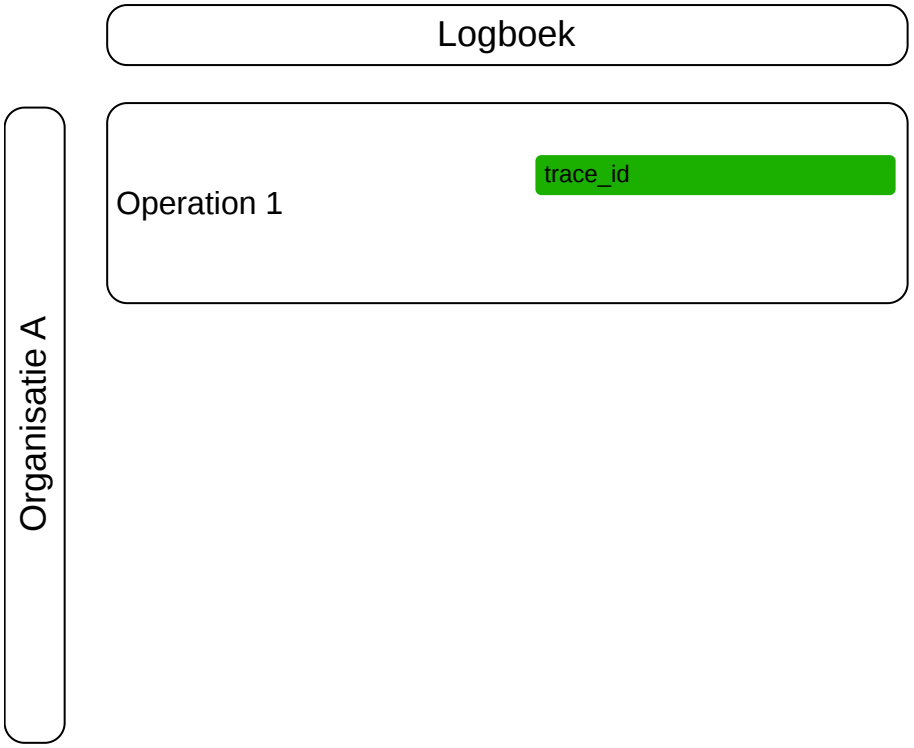
Bij het verstrekken van deze data aan de aanvragende organisatie, wordt het `processing_activity_id` van de gegevensverstrekkende organisatie geregistreerd. Er is dus GEEN rechtstreekse koppeling tussen het Register van de aanvragende en het Register van de verstrekkende organisatie.

Figuur 7 Afbeelding relaties processing_activity_id tussen Logboek en Register bij meerdere organisaties

3.3 trace_id als grootste gemene deler

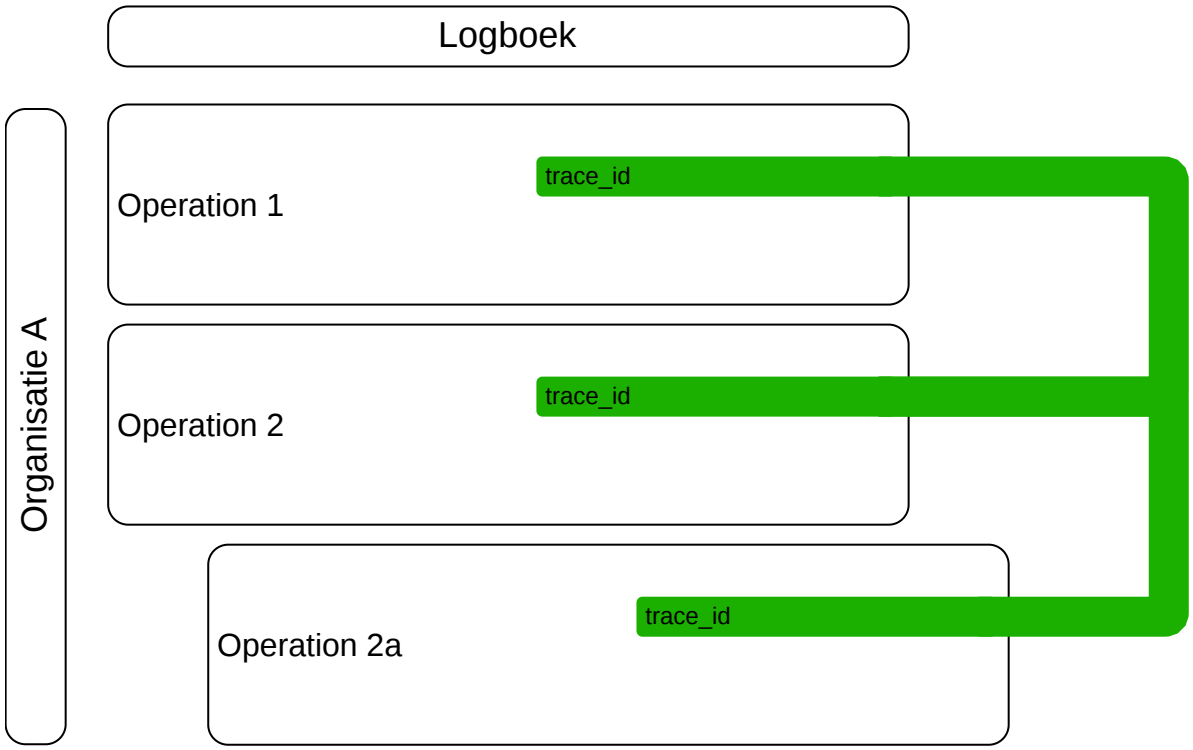
Operations kunnen bestaan uit meerdere (sub)Operations binnen de eigen organisatie maar ook over organisaties heen. Het geheel kan een grote en ingewikkelde constructie worden. Om toch het overzicht te kunnen behouden, is het noodzakelijk een `trace_id` te introduceren per (sub)Operation.

Het `trace_id` is als het ware de 'lijm' tussen alle (sub)Operations. Als er nog geen `trace_id` bekend is, wordt deze automatisch gegenereerd voor de eerste Operation.



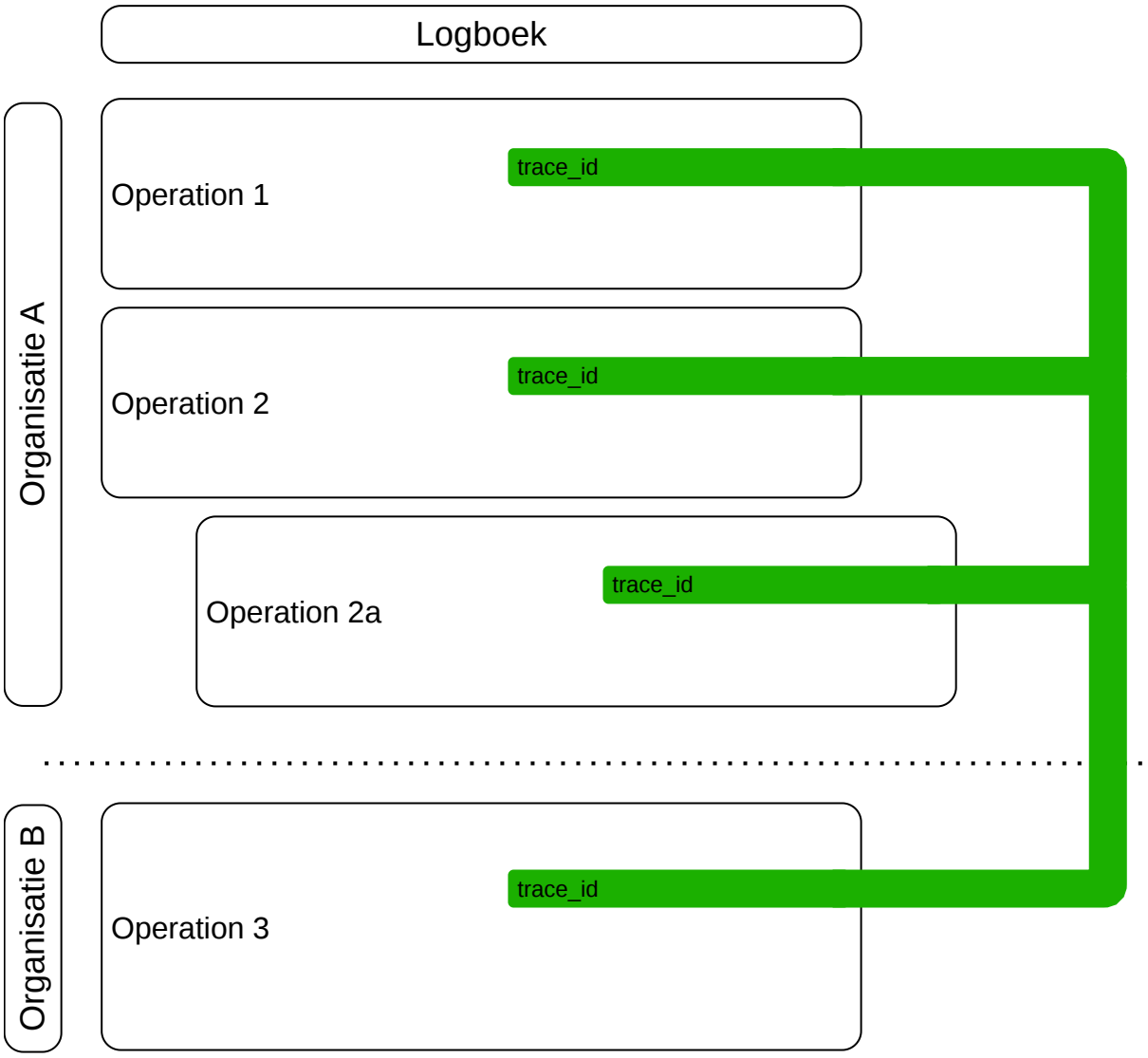
Figuur 8 Afbeelding trace_id

Alle bij elkaar horende (sub)Operations, krijgen vervolgens dezefde `trace_id`-waarde.



Figuur 9 Afbeelding relaties trace_id

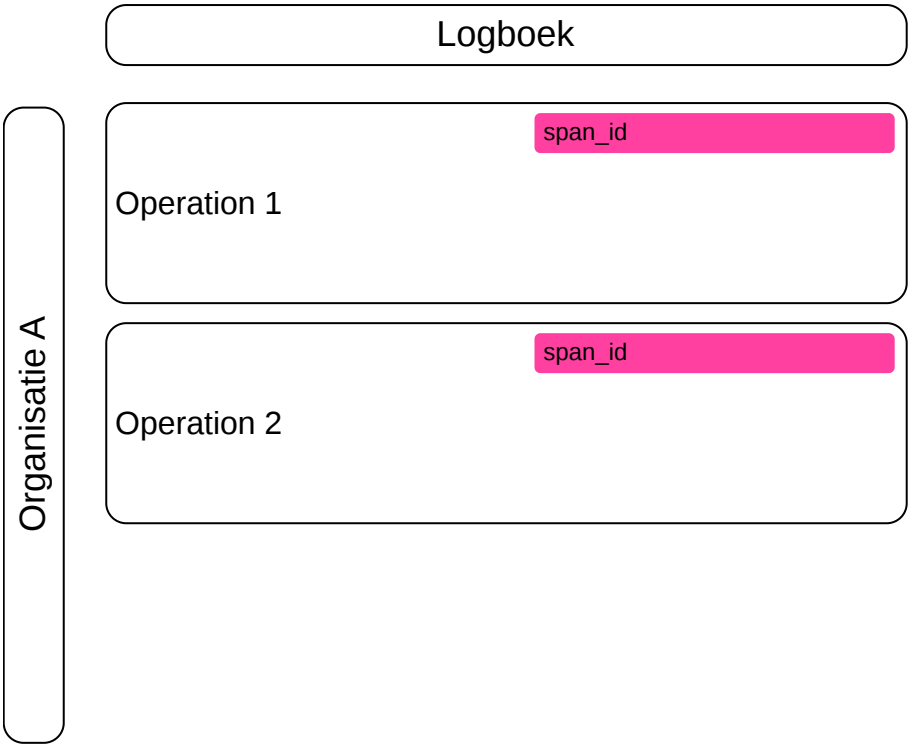
In het geval dat er data wordt opgevraagd aan een andere organisatie, geeft de vragende organisatie de `trace_id` door aan de verstrekkende organisatie. De `trace_id` is identiek bij beide organisaties, waardoor er een relatie te leggen is tussen de verwerkingen van de vragende en de verstrekkende organisatie.



Figuur 10 Afbeelding relaties trace_id en meerdere organisaties

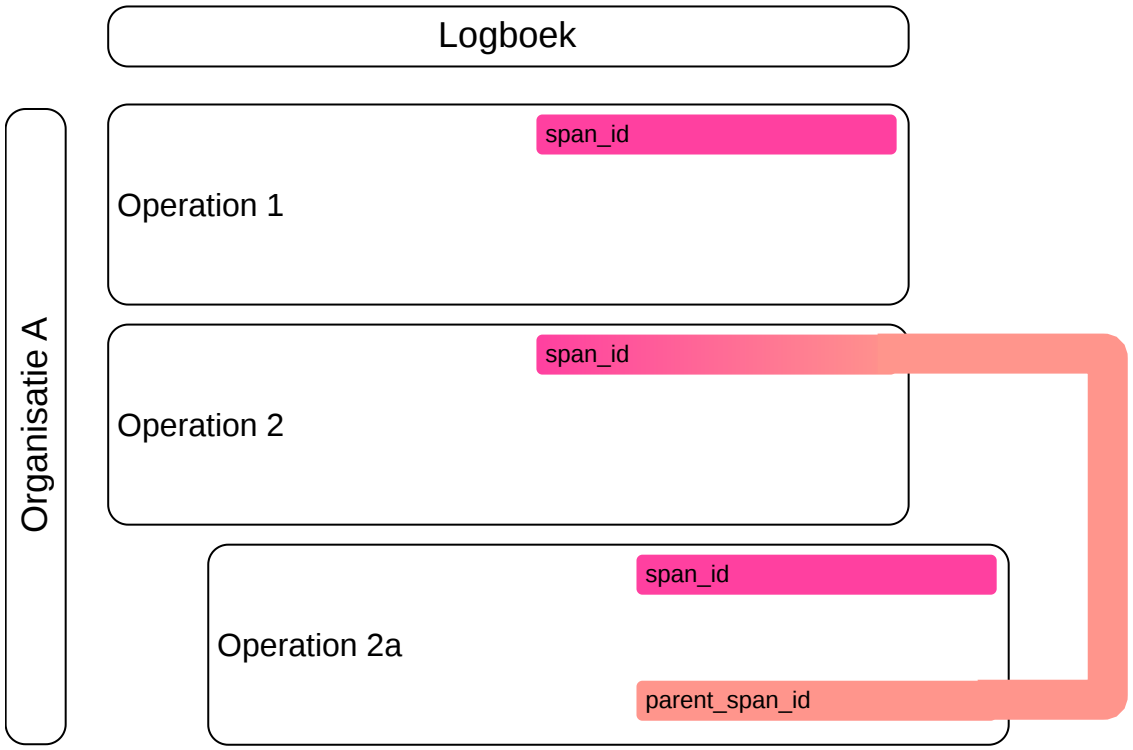
3.4 Relatie tussen (sub)Operations

Elke (sub)Operation krijgt een eigen, unieke `span_id`. Hiermee zijn alle loggings altijd uniek traceerbeer. Ook subOperations krijgen een eigen, unieke `span_id`.



Figuur 11 Afbeelding span_id

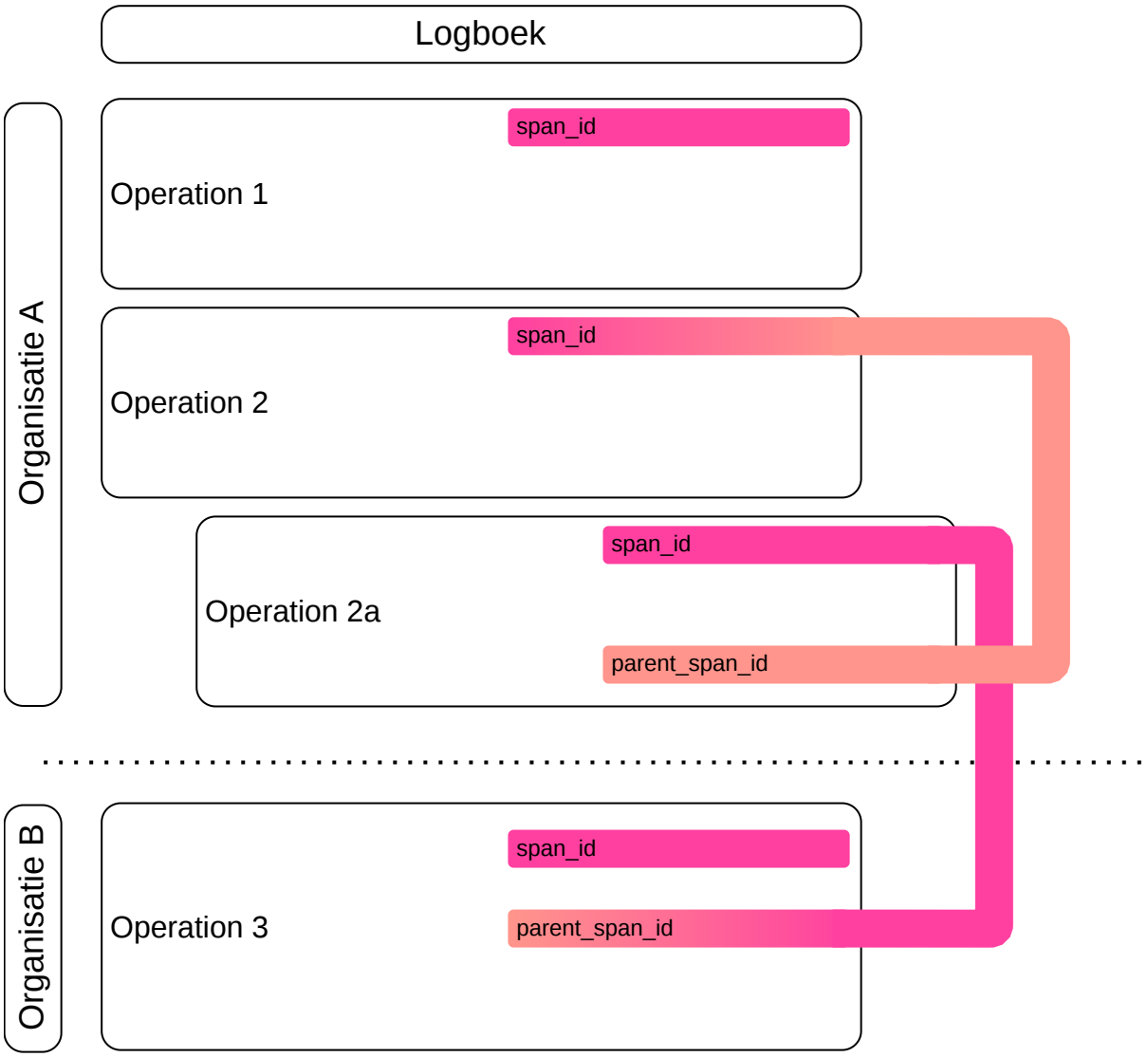
Als er ook subOperations plaatsvinden, moet er ook een `parent_span_id` worden geregistreerd om de koppeling met de hoofdOperation te realiseren.



Figuur 12 Afbeelding span_id en parent_span_id

In het geval er data nodig is van een andere organisatie, krijgt de Operation van de verstrekkende organisatie ook een eigen, unieke `span_id`.

Daarnaast wordt bij deze Operation ook het `span_id` geregistreerd die het verzoek voor informatie geïnitieerd heeft (vanuit de vragende organisatie). Deze specifieke `span_id` wordt het `parent_span_id` genoemd en krijgt de waarde gelijk aan het `span_id` van de initiërende Operation van de vragende organisatie.



Figuur 13 Afbeelding span_id en parent_span_id

3.5 Voorbeeld van een traceringsconstructie

Het nu volgende voorbeeld is volledig fictief en is puur bedoeld om een beeld te schetsen ten behoeve van een traceringsconstructie in een logboek.

§ 3.5.1 Situatieschets

Een persoon heeft een parkeervergunning in een gemeente. Er is een nieuwe auto aangeschaft, het kenteken moet worden aangepast ten behoeve van de vergunning. De persoon kan het kenteken online wijzigen in de 'mijnGemeente' applicatie. Om het voorbeeld eenvoudig te houden, worden foutsituaties buiten beschouwing gelaten.

§ 3.5.2 Procesgang

1. Persoon logt in gemeenteapplicatie.
2. Gemeente toont huidige parkeervergunning.
3. Persoon wijzigt kenteken in de gemeenteapplicatie.
4. Gemeenteapplicatie vraagt het RDW om data op basis van de tenaamstelling.
5. RDW geeft de gevraagde data terug aan de gemeenteapplicatie.
6. Gemeenteapplicatie accepteert de wijziging van de persoon.

De traceringsdata worden als volgt vastgelegd:

§ 3.5.3 processing_activity_id

In de gemeenteapplicatie worden de volgende Operations uitgevoerd die een relatie hebben met het Register van Verwerkingsactiviteiten van de gemeente:

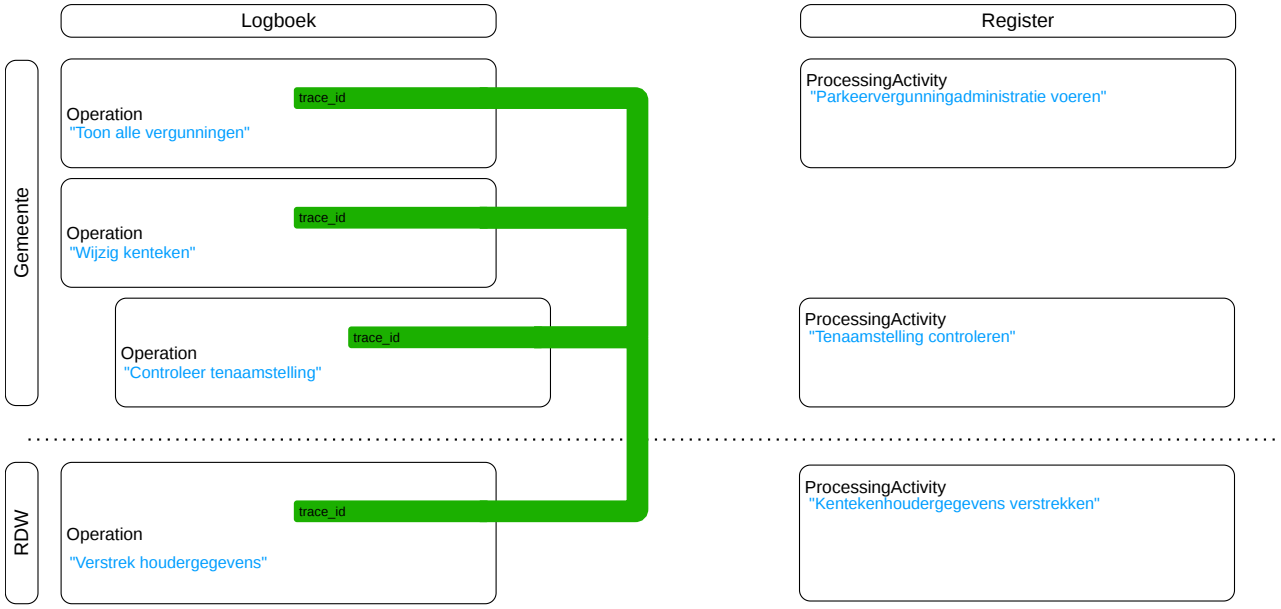
- **Toon alle vergunningen**: na het inloggen, worden de parkeervergunningen van de persoon getoond. Deze Operation is gerelateerd aan de processingActivity **Parkeervergunningadministratie voeren**.
- **Wijzig kenteken**: het wijzigen van het kenteken valt ook onder de processingActivity **Parkeervergunningadministratie** voeren. Hierdoor is het `processing_activity_id` hetzelfde als die van de Operation **Toon alle vergunningen**.
- **Controleer tenaamstelling:** deze Operation zorgt voor de aanvraag van data richting het RDW en controle van de terugontvangen data. Deze Operation is een subOperation van **Wijzig kenteken** en krijgt een processingActivity wat hoort bij de processingActivity in het Register genaamd **Tenaamstelling controleren**. De processingActivity is op zijn beurt weer een subprocessingActivity van **Parkeeradministratie voeren**.

In de RDW-applicatie wordt het verstrekken van data aan de gemeenteapplicatie ook geregistreerd. De Operation **Verstrek houdergegevens** is gerelateerd aan de processingActivity **Kentekenhoudergegevens verstrekken**. Merk op dat er hier dus GEEN directe relatie is tussen het Register van Verwerkingsactiviteiten van de gemeente en die van het RDW.

Figuur 14 Afbeelding voorbeeld processing_activity_id bij Gemeente en RDW

§ 3.5.4 trace_id

- De gemeenteOperations **Toon alle vergunningen, Wijzig kenteken en Controleer tenaamstelling** behoren tot dezelfde handeling (met als eindresultaat het wijzigingen van het kenteken op de vergunning). Deze Operations krijgen allemaal dezelfde `trace_id`.
- De RDW-Operation **Verstrek houdergegevens** krijgt een eigen `trace_id`.
- Om het geheel te koppelen over de organisaties heen, wordt bij het RDW ook een `trace_id` opgeslagen, de waarde hier van is gelijk aan de waarde van de `trace_id` van de Operation **Controleer tenaamstelling**.

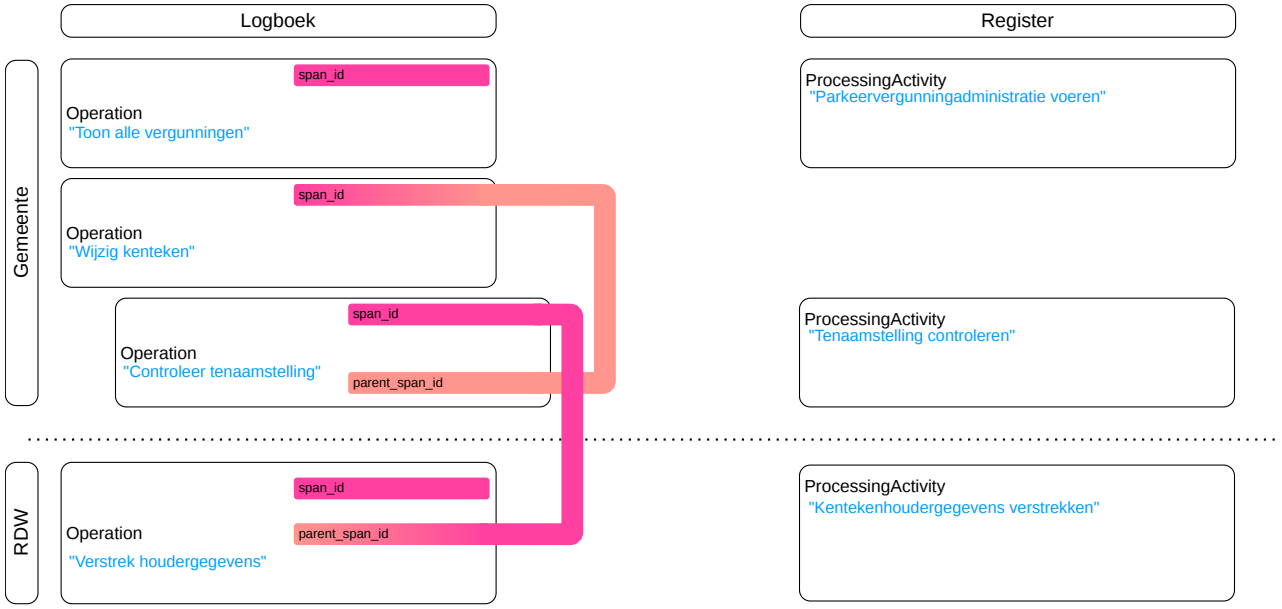


Figuur 15 Afbeelding trace_id bij Gemeente en RDW

§ 3.5.5 span_id

In de gemeente-applicatie krijgt elke (sub)Operation een eigen, unieke `span_id`.

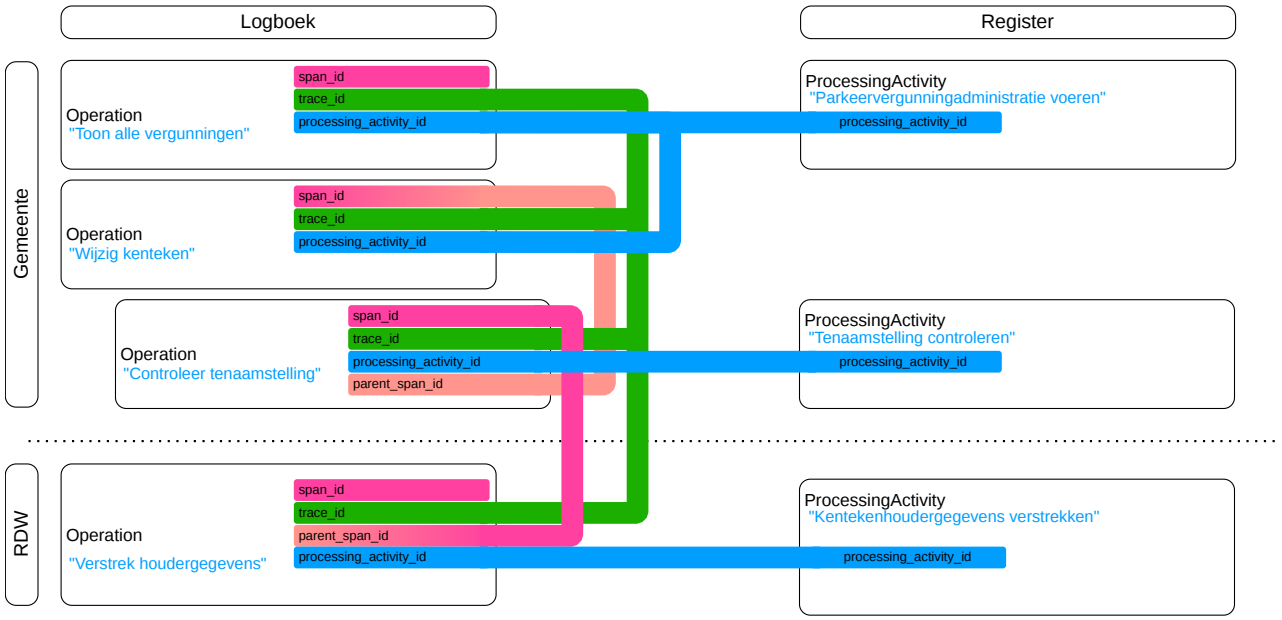
- De (sub)Operation **Controleer tenaamstelling** krijgt daarnaast ook nog een `parent_span_id` met de waarde van `span_id` van de **Operation Wijzig** kenteken om een relatie te leggen.
- Ook de RDW-Operation **Verstrek houdergegevens** krijgt een eigen unieke `span_id`.
- Om de relatie over de organisaties heen te leggen, wordt er bij de RDW-Operation **Verstrek houdergegevens** ook een `parent_span_id` moeten worden vastgelegd. De waarde van deze `parent_span_id` is gelijk aan de waarde van de `span_id` van de gemeente-Operation **Controleer tenaamstelling**.



Figuur 16 Afbeelding voorbeeld span_id en parent_span_id bij Gemeente en RDW

§ 3.5.6 Totaalbeeld

Als alle relaties gelegd zijn, ziet de traceringsconstructie er als volgt uit:



Figuur 17 Afbeelding Voorbeeld met alle span, trace en processing elementen

Meer gedetailleerde voorbeelden staan beschreven op developer.overheid.nl.

↥