



Rijksdienst voor Identiteitsgegevens
*Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties*

Vragenuurtje BRP API



Thema van vandaag: autorisatie, logging, protocollering

Binnengekomen vragen:

1. Hoe werkt het proces voor het toetsen of een taakspecifieke applicatie geautoriseerd mag worden voor BRP API bevestigingen?
2. En hoe wordt dat per applicatie geconfigureerd welke set van gegevens ze mogen verwerken?
3. Wanneer alle vak applicaties gebruik maken van de BRP API, hoe houden we dan bij welke personen een applicatie wil volgen?
4. Graag iets meer vertellen over monitoring en logging. Welke afwegingen moeten we als organisatie maken?
5. Hoe sluit dit aan op gemeentelijke logging (zoals ENSIA-verplichtingen)?



Stelselpedia > BRP-index

Autorisatie

Algemeen

Per registratie met niet-openbare gegevens regelt een organisatie (landelijke of gemeentelijke verstrekker of afnemer) wie toegang heeft, tot welke gegevens en voor welke taken, volgens een vastgesteld autorisatieproces.

In het geval van de BRP gaat het om persoonsgegevens.



Voor de BRP zijn de volgende autorisatieprocedures van toepassing:

- Autorisatieformulier toegang Amsterdamse en landelijke distributievoorziening BRP
- Autorisatieformulier sFTP

Voor de formulieren wordt verwezen naar de [productenpagina](#) van de registratie ingezetenen.

Vraag 1: Autorisatie

1. B&W = verstrekker BRP gegevens (niet RvIG!)
2. Raadpleegt hiervoor de BRP via de BRP API
3. Voor zowel binnen- als buitengemeentelijke personen
4. GABA autorisatie: raadplegen buitengemeentelijke personen mag alleen voor de wettelijke taken die in GABA genoemd zijn. "Kruisjeslijst" is niet meer van toepassing



Gefaseerd security opschalen

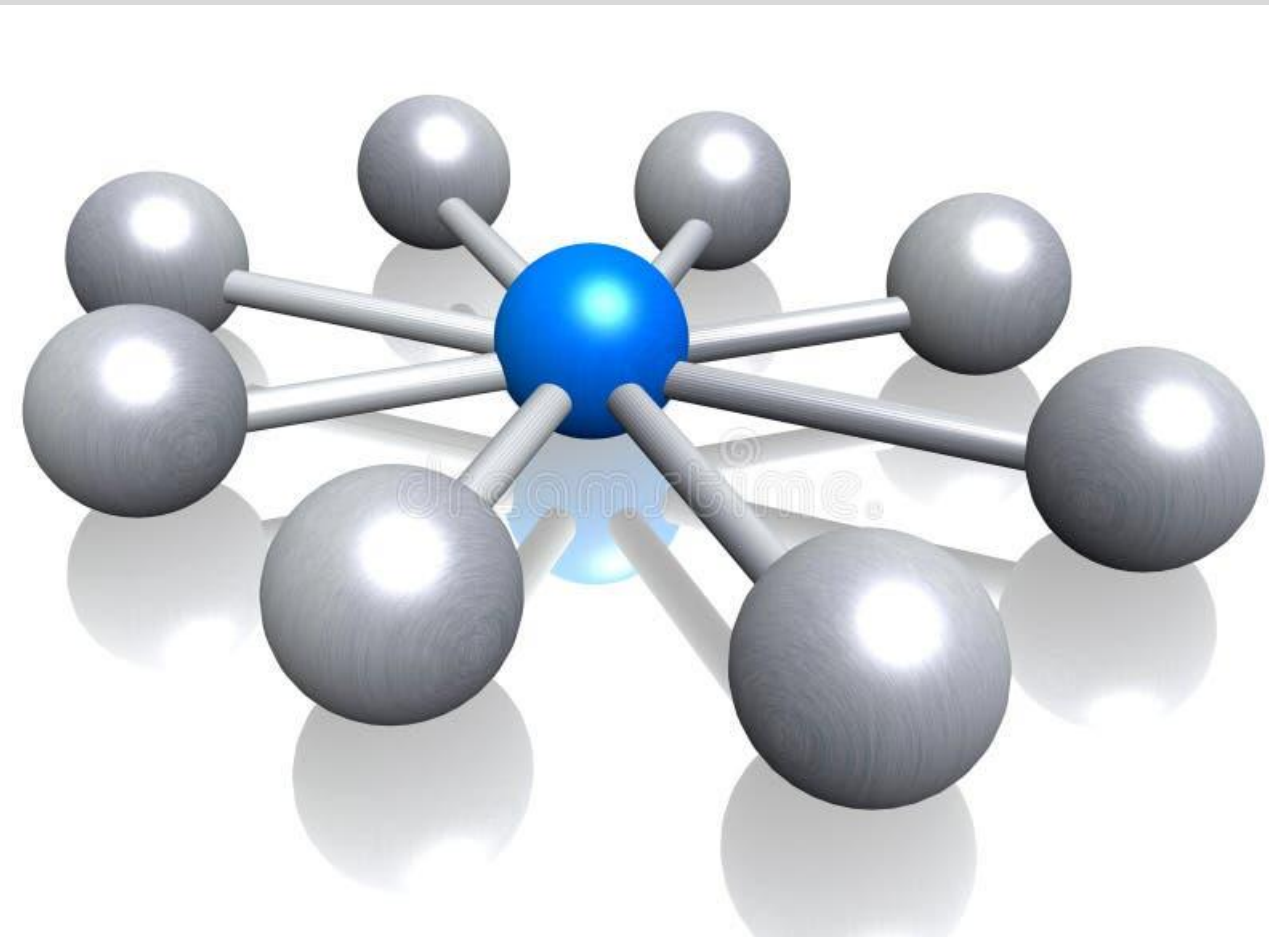
- (Toegangs)beveiliging, autorisatie en filtering (verplicht)
- Logging- en protocollering: controle achteraf en misbruik voorkomen (verplicht)
- IGA-systeem: beheren van identiteit, rollen en rechten (optioneel)

Lees meer op:
realisatie.github.io/Haal-Centraal/security



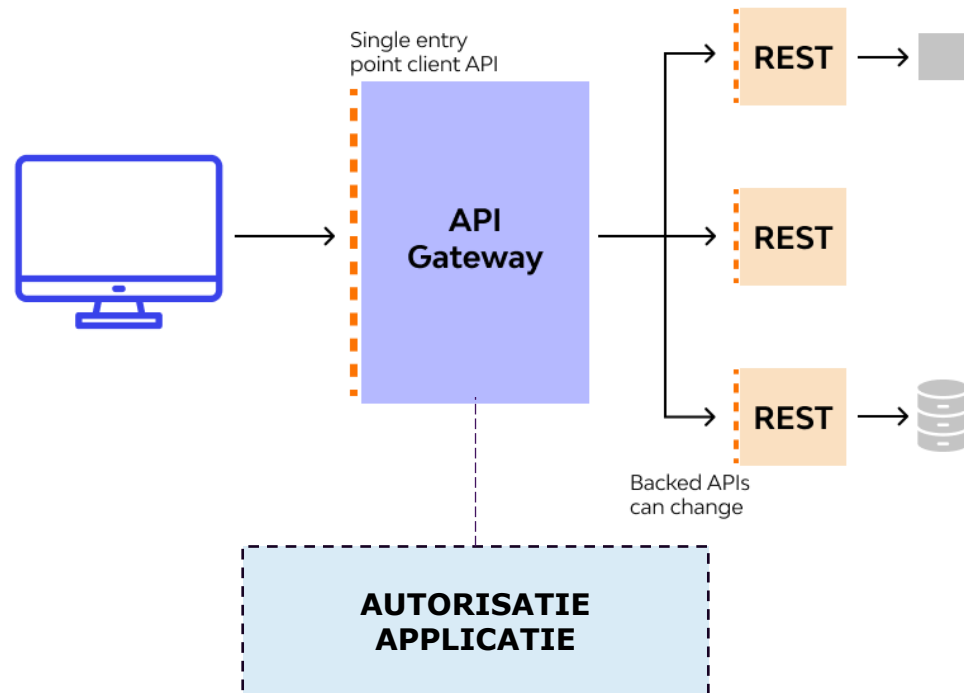
Transitie

- VAN: alle security in de taakapplicatie
- NAAR: security in door organisatie gecontroleerde centrale voorzieningen





Vraag 2: hoe autorisatie configureren?



- Autorisatiefiltering door API Gateway (gemeente Amsterdam)

OF

- Autorisatiefiltering door autorisatie applicatie (gemeente Den Haag)

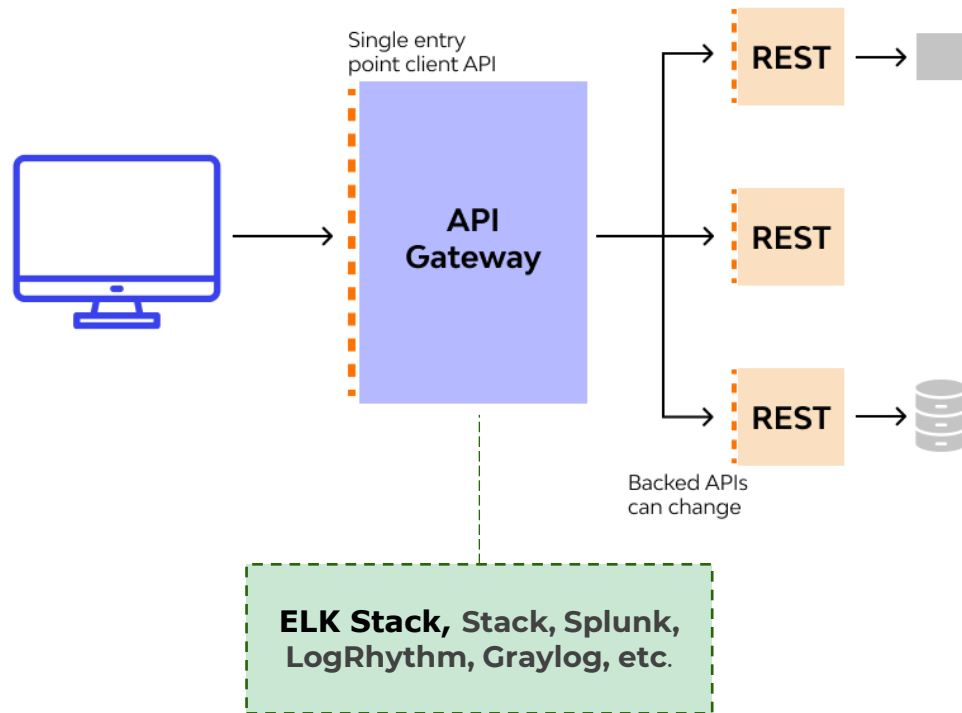


Vraag 3: Hoe bijhouden welke app welke personen volgt?

- Notificatie API
 - in ontwikkeling
 - gepland voor 1 jan 2026
 - We doen ons best de systematiek voor gemeenten te vereenvoudigen



Vraag 4: Logging



- Protocolleren
 - van verstrekkingen
 - is verplicht
 - Request opslaan, met timestamp en identiteit en rol bevrager (voor welke wettelijke taak/autorisatie)
 - Uit de response alleen de BSN opslaan
 - zowel voor zoek- als raadpleegvragen
 - 20 jaar bewaren
 - ten behoeve van een burgerverzoek
- Logging
 - voor beheerdoeleinden en onderzoek privacy officer/ security officer. Indien response wordt opgeslagen, goed beveiligen!
- Centraal loggen binnen gemeente via API Gateway
- Centraal opslaan & analyseren in bijv. ELK stack, Splunk etc.



Thema van vandaag: logging & protocollering

5. Hoe sluit dit aan op gemeentelijke logging (zoals ENSIA-verplichtingen)?

Gemeentelijke logging: wij adviseren de verstrekking van alle privacygevoelige gegevens binnen de gemeente centraal te loggen op de in deze presentatie beschreven manier. ENSIA is een verantwoordingsinstrument/ audit, waarbij je de gestelde vragen beantwoordt zoals je dat ook doet voor het gebruik van de ad-hoc webservice en spontane verstrekkingen van RvIG.



ATRIUM
city hall

EVENT SHOWCASE Haal Centraal DEN HAAG
14 mei, is jouw IT management erbij?



Extra informatie

- [Meer informatie over de BRP API \(RvIG.nl\)](https://RvIG.nl)
- Technische specificaties Git-Hub
 - [BRP API Personen](#)
 - [BRP API Bewoning](#)
 - [BRP API Verblijfplaats historie](#)



Overige Vragen

- › Hoe zit het met persoonsgegevens die voor een bepaalde taak helemaal niet nodig zijn?

Antwoord:

Een taaksysteem of medewerkers met een rol die aan een wettelijke taak is gekoppeld worden uitsluitend geautoriseerd voor de gegevens die zij nodig hebben. Deze autorisatie wordt afgedwongen door een zgn "proxy" op de API Gateway of een applicatie die de autorisaties van binnengemeentelijke afnemers handhaaft (zie antwoord vraag 2)



Overige Vragen

- › Hoe bepaal je welke persoonsgegevens? In relatie met de AVG? In de praktijk zal ik dan terugvallen op de "kruisjeslijst" van de GABA.

Antwoord:

Een taaksysteem of medewerkers met een rol die aan een wettelijke taak is gekoppeld worden uitsluitend geautoriseerd voor de gegevens die zij nodig hebben. Om deze set te bepalen is het nodig je te verdiepen in het proces van de afnemer met de wettelijke taak.

Wij snappen dat de GABA een startpunt kan zijn, maar bedenk dat er ook taken zijn die nu niet in de GABA voorkomen omdat het alleen om het bevragen gegevens van eigen inwoners gaat (altijd al een gemeentelijke verstrekking). Bovendien kan gemeentelijke wetgeving per gemeente anders zijn.

De gemeente is verstrekker, en daarmee verantwoordelijk voor de autorisatie.



Overige Vragen

- › GABA zal dus ook vervallen uiteindelijk?

Antwoord:

Dat is zeker mogelijk. In het experiment is de rol van de GABA al veranderd, en er moet een goede reden zijn om dit terug te draaien in nieuwe wetgeving. Het huidige kader met twee verstrekkers wordt bovendien als complex ervaren.



Overige Vragen

- › Moet je ook kunnen aantonen dat je na 20 jaar de protocollering hebt vernietigd? Dus moet er toch nog iets bewaard blijven? Of mag het echt weg?

Antwoord:

Het mag echt weg, hoeft geen bewijs van bewaard te worden. Maar je moet het wel 20 jaar bewaren



Overige Vragen

- › Dient alleen het request of moet ook het antwoord bericht worden bewaard?

Antwoord:

Alleen het request, samen met de BSN(s) uit het antwoord . Je mag ook het hele antwoord opslaan voor loggingdoeleinden voor zolang als dat nodig is, maar dat moet wel heel goed beveiligd worden



Overige Vragen

- › Welke afspraken zijn er met betrekking tot wat je moet loggen. En wat je niet mag loggen? BSN bijvoorbeeld? Eigenlijk ben ik op zoek naar een soort best practice.

Antwoord:

Het minimale is het request, samen met de BSN(s) uit het antwoord (zie vraag 4), rest is aan de verstrekker



Overige Vragen

- › Zijn er gemeenten die voor verschillende verstrekkingen een wettelijke grondslag met doelbinding hebben bepaald die (als basis) door andere gemeenten gebruikt kunnen worden. Iedere gemeente kan dat zelf bepalen, maar zouden niet allemaal het wiel hoeven uit te vinden. Den Haag, Amsterdam?

Antwoord:

Ja zeker, daar zou een rol voor de VNG zijn weggelegd, maar met elkaar delen en hierover het gesprek aan te gaan is een heel goed idee. Brenda geeft aan dat zij het van de gemeente Den Haag op een later moment kan delen.



Overige Vragen

- › Worden API Gateway leveranciers getoetst door jullie?

Antwoord:

Nee, we willen wel weten of en welk product eronder zit. Alle leveranciers in het overheidsdomein die diensten verlenen op een API Gateway gebruiken daarvoor een product (Layer7, WSO2) dat in de markt bekend is, en is beoordeeld door bijvoorbeeld Gartner. Toetsen is tot nu toe niet nodig geweest.



Overige Vragen

- › Is er dan een overzicht van alle op dit moment ondersteunde API Gateways?

Antwoord: Nee, maar ik weet wel welke Gateways voor de BRP API worden gebruikt:

- › *Enable-U: layer7 APOI Gateways (Broadcom)*
- › *Pink Roccade en Yenlo: WSO2 API Manager (Open Source)*
- › *Gemeente Amsterdam: API Management (Microsoft)*



Overige Vragen

- › Hoe kunnen we de vorderingen cq ontwikkelingen van de notificatie service volgen?

Antwoord:

Via de DevPortal – github. Er komt binnenkort een github repo en een aankondiging op de DevPortal. Deze wordt overigens binnenkort vernieuwd!



Overige Vragen

- › Zijn er gemeenten die afwijken van de GABA-besluiten van de RvIG? Wij vonden die altijd leidend. → Wij volgen ook het GABA-autorisatiebesluit

Antwoord:

Van oudsher gaat het college over wat er wordt verstrekt over eigen inwoners. Onderzoek naar grondslag is belangrijk, zeker als het om lokale wetgeving gaat. GABA besluiten gaan alleen over taken waarvoor buitengemeentelijke personen moeten worden geraadpleegd, en dekken niet alle dienstverlening af. Het kan een startpunt zijn, maar is niet toereikend.



Overige Vragen

- › Leg je dit dan voor aan het college? Of wie beslist er dan over?

Antwoord gemeente Den Haag:

B&W besluit