

Plan van Aanpak: gemeentelijke samenwerking IRMA

1. Aanleiding

De VNG heeft in het jaarprogramma van het Gezamenlijk Gemeentelijk Uitvoeringsfonds 2019 digitale identiteit als speerpunt benoemd als ‘gemeenschappelijke basis voor de toekomst’¹. De drie elementen van deze digitale identiteit zijn in 2018 omschreven in een position paper².

Uitgangspunten digitale identiteit:

- Identificatie en authenticatie in alle contexten en langs alle kanalen*
 - Accordering en ondertekening van stukken of transacties, zodat deze rechtsgeldig zijn en voldoende betrouwbaar in het maatschappelijk verkeer tot op het hoogste niveau*
 - regie op gegevens (en diensten die de burger afneemt)*
-

Om te onderzoeken of het mogelijk is handen en voeten te geven aan deze uitgangspunten is er in de tweede helft van 2018 een identiteitslab georganiseerd door de VNG in samenwerking met het ministerie van Binnenlandse Zaken en Koninkrijksrelaties en onderzoeksinstituut WAAG³.

In het kader van dit identiteitslab heeft de gemeente Nijmegen een verstrekking uit de basisregistratie personen (BRP) gerealiseerd via IRMA (I Reveal My Attributes)⁴. Uit het onderzoek van het identiteitslab blijkt dat IRMA tevens voldoet aan de uitgangspunten, zoals verwoord in de position paper. In de tussentijd heeft IRMA de Brouwerprijs voor Wetenschap en Samenleving⁵ ontvangen en is het door Internet Society Nederland uitgeroepen tot beste internetinnovatie van 2019⁶.

Om IRMA in 2019 naar een landelijk niveau te tillen en het gebruik te stimuleren, is het noodzakelijk dat de meest relevante gegevens, die uit de basisregistratie personen, landelijk beschikbaar te maken op een hoog betrouwbaarheidsniveau.

2. Over IRMA

*IRMA, I Reveal My Attributes, is een privacy vriendelijk identiteitsplatform voor zowel authenticatie als ondertekening*⁷. Dit staat vermeld op de site van de Privacy by Design Foundation, die zicht richt op de ontwikkeling en het gebruik van IRMA.

2.1 Stichting Privacy by Design

De stichting en het platform zijn ontstaan vanuit de studiegroep ‘digital security’ aan de Radboud Universiteit. Deze studiegroep heeft onderzoek gedaan naar identificatie en autorisatie in de digitale wereld. Hierbij kwam men uit op het principe van een ‘attribuut gebaseerde’ identiteit. Dat wil zeggen dat ieder stukje van je persoonsgegevens als ‘attribuut’ gepresenteerd kan worden: bijvoorbeeld je geboortedatum. Om het zo los te knippen van alle andere

¹ <https://vng.nl/onderwerpenindex/bestuur/brieven/alv-voorstel-gezamenlijke-gemeentelijke-uitvoering-2019>

² <https://vng.nl/onderwerpenindex/dienstverlening-en-informatiebeleid/dienstverlening-aan-inwoners-en-ondernemers/nieuws/vng-position-paper-digitale-identiteit>

³ <https://digitaleidentiteit.waag.org/>

⁴ <https://tweakers.net/nieuws/143823/nijmegen-test-identificatieapp-irma-die-privacy-waarborgt.html>

⁵ <https://www.khmw.nl/privacy-by-design-ontvangt-brouwer-prijs-2018/>

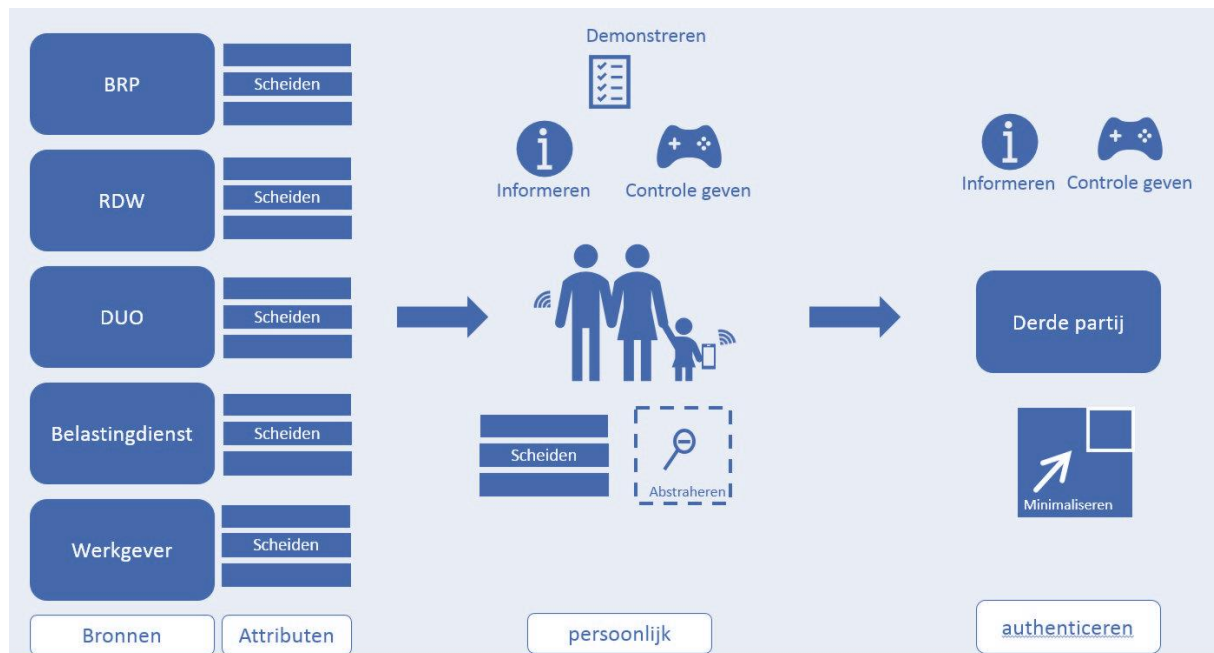
⁶ <https://awards.isoc.nl/innovatie/2019/>

⁷ <https://privacybydesign.foundation/irma/>

persoonsgegevens, wordt het al een stukje minder privacy gevoelig. Ook kun je dit 'attribuut' aggregeren. Een persoon geboren op 10 augustus 1987 is ouder dan 12, 16 en 18, maar jonger dan 67 en 4 maanden (leeftijden met een wettelijke betekenis). Alleen het gegeven 'ouder dan 18' is helemaal privacy vriendelijk.

2.2 Attribuut gebaseerde identiteit

De IRMA omgeving maakt het mogelijk om vanuit bestaande registraties, zoals de BRP⁸ en het BIG-register, je eigen gegevens op te vragen en om te zetten in attributen. Deze attributen kun je op een later tijdstip in de digitale wereld inzetten om je te authenticeren. Indien je alcoholische drank wil kopen op internet hoeft je zodoende alleen je adres door te geven en het attribuut 'ouder dan 18'. De webshop weet op dat moment dat de alcohol verkocht mag worden zonder dat zij te veel informatie over je uitvragen. Dit principe staat uitgelegd in onderstaande afbeelding:



Centraal in van de afbeelding staat de persoon. Vanuit gevalideerde en betrouwbare bronnen ontvangt deze attributen, dit kunnen gegevens zijn uit de Basisregistratie Personen (BRP) zoals naam, adres en geboortedatum, maar ook gegevens vanuit de werkgever zoals 'werkzaam als' of 'bruto salaris'. Deze attributen worden gescheiden van elkaar aangeleverd aan de persoon en waar mogelijk geabstraheerd (bijvoorbeeld salaris boven minimumloon). De persoon kan deze attributen vervolgens verstrekken aan een derde partij om er 'iets mee te doen' (bijvoorbeeld aan een bank om een hypotheek aan te vragen).

2.2.1 Credentials en attributen

Om enige structuur aan te brengen in 'het woud' van attributen zit er enige structuur in de attributen. Een setje attributen dat bij elkaar hoort wordt een 'credential' genoemd. Voorbeeld:

CREDENTIAL:	PERSONALDATA
ATTRIBUUT:	VOORNAMEN
ATTRIBUUT:	TUSSENVOEGSEL
ATTRIBUUT:	ACHTERNAAM
ATTRIBUUT:	ADELLIJKE TITEL

⁸ Basisregistratie personen

Dit heeft als voordeel dat een gebruiker deze ‘setjes attributen’ in een keer kan ophalen, maar per attribuut kan verstrekken. Dit bevordert het gebruiksgemak voor de gebruiker en biedt een maximale variant van ‘privacy by design’.

2.3 Digitaal ondertekenen

Met de IRMA-functionaliteit is het tevens mogelijk om een digitale handtekening te zetten. De eIDAS verordening stelt de volgende eisen aan een digitale handtekening:

1. De handtekening is op een unieke wijze aan de ondertekenaar verbonden;
2. De handtekening maakt het mogelijk om de ondertekenaar te identificeren;
3. De handtekening komt tot stand met gegevens voor het aanmaken van elektronische handtekeningen die de ondertekenaar, met een hoog vertrouwensniveau, onder zijn uitsluitende controle kan gebruiken en
4. De handtekening is op zodanige wijze aan de daarmee ondertekende gegevens verbonden, dat elke wijziging achteraf van de gegevens kan worden opgespoord.

Dit gaat verder dan het authenticeren, zoals in de vorige paragraaf omschreven. In tegenstelling tot het betrouwbaar authenticeren, dat binnen de overheid kan met DigiD en buiten de overheid met accounts van onder andere Google en Facebook, is digitaal ondertekenen niet breed mogelijk conform de 4 bovengenoemde punten. De IRMA-app biedt functionaliteit om middels attributen een handtekening te plaatsen die dit wel mogelijk maakt.

2.4 Huidige situatie: kip – ei probleem

Momenteel heeft de stichting Privacy by Design last van het ‘kip – ei probleem’. De app en de achterliggende techniek om attributen te verkrijgen en te verstrekken zijn klaar, maar er zijn nog weinig attributen beschikbaar, waardoor er nog maar weinig partijen zijn die IRMA kunnen gaan gebruiken. Andersom: er zijn maar weinig partijen die IRMA gebruiken, waardoor het voor ‘uitgevers van attributen’ geen meerwaarde heeft om attributen uit te geven.

3. Wat vooraf ging

Tijdens de werkconferentie in het kader van het programma open en weerbaar op 12 maart 2018 is de gemeente Nijmegen in aanraking gekomen met de stichting Privacy by Design en heeft kennis genomen van het eerder beschreven kip – ei probleem. Aangezien de principes achter IRMA onderschreven worden door de gemeente Nijmegen, is besloten om een proof of concept te maken voor het leveren van BRP attributen via IRMA.

3.1 Juridische basis

Allereerst is onderzocht of er een juridische basis is voor het leveren van gegevens uit de BRP via IRMA. Deze blijkt er te zijn conform artikel 2.55 lid 1 Wet BRP:

HET COLLEGE VAN BURGEMEESTER EN WETHOUDERS DEELT EEN IEDER OP DIENS VERZOEK SCHRIFTELIJK BINNEN VIER WEKEN KOSTELOOS MEDE OF HEM BETREFFENDE PERSOONSgegevens IN DE BASISREGISTRATIE WORDEN VERWERKT. INDIEN ZODANIGE GEGEVENS WORDEN VERWERKT, WORDT DE VERZOEKER MET BETREKKING TOT DE BASISREGISTRATIE DE IN ARTIKEL 2.54, DERDE LID, BEDOELDE SCHRIFTELIJKE MEDEDELING GEDAAN.

Kortom: de gemeente verstrekt kosteloos en op een begrijpelijke wijze de gegevens die over een inwoner in de BRP staan.

Uit de memorie van toelichting van de wet BRP blijkt dat dit niet alleen van toepassing is voor gegevens van inwoners van de eigen gemeente, maar van alle ‘ingeschrevenen’ in de BRP. Kortom: van alle inwoners van Nederland. In combinatie met artikel 20 van de Algemene verordening gegevensbescherming (AVG) die voorschrijft dat dit gedaan moet worden op een wijze waardoor het voor betrokkene makkelijk is om de gegevens her te gebruiken, dataportabiliteit, maakt het een verstrekking via IRMA bijna noodzakelijk.

Dit is bevestigd door zowel gemeentelijke experts als door de Rijksdienst voor Identiteitsgegevens, de beheerder van de GBA-v en maakt de weg vrij om gegevens te verstrekken aan inwoners van Nederland via IRMA.

3.2 Technische Proof of Concept

Vervolgens is gestart met een technische Proof of Concept (hierna PoC). Deze PoC heeft zich gericht op 3 facetten: het uitgeven van attributen uit de test GBA-v achter DigiD, een pre-fill demopagina maken op Nijmegen.nl met IRMA attributen en ondertekening in de testomgeving mogelijk maken met IRMA attributen. Daarnaast is in de PoC meegenomen dat er relaties opgebouwd worden met landelijke partijen om IRMA mee te ontwikkelen.

3.2.1 Uitgeven attributen

In de PoC is het gelukt om attributen te verstrekken vanuit de test GBA-v achter test DigiD. Hiervoor zijn een aantal services gebouwd en is een verbinding gemaakt tussen de IRMA app en Nijmegen.nl.

3.2.2 Pre-fill demopagina

De pagina: https://www.nijmegen.nl/gns/no_index/irma/demo/ staat online. In deze pagina kan middels reeds beschikbare IRMA attributen een webformulier worden gevuld. Tevens is er een pagina gemaakt die ingevuld kan worden met de test BRP gegevens. Ook bij deze pagina's ontbreekt het nog aan de nodige veiligheidsmaatregelen.

3.2.3 Ondertekening

Er is een demopagina gemaakt om een terugbelverzoek te doen met een IRMA ondertekening. Hierbij moet worden opgemerkt dat de software aan de kant van IRMA nog moet worden verbeterd. De vraag 'ik wil teruggebeld worden op nummer 06-12345678' die moet worden bevestigd via IRMA komt nog niet in een mooi leesbaar formaat binnen op de app.

3.3 Van Proof of Concept naar Pilot

Nadat gebleken is dat de drie zaken uit de PoC succesvol uitgevoerd konden worden, is er gestart met het daadwerkelijke verstrekken van gegevens uit de BRP, aangezien hier de grootste meerwaarde bestaat die als overheid geleverd kan worden.

Op 26 september 2018, tijdens het Fieldlab Dienstverlening, is de verstrekking van gegevens uit de BRP van start gegaan. Tot 30 januari is er ruim 2.000 keer gebruik gemaakt van deze service.

4. Probleemstelling

De gemeente Nijmegen heeft al bij de start van de uitgifte van de gegevens uit de BRP aangegeven dat dit gedaan wordt bij wijze van pilot en dat direct gezocht wordt naar een landelijke partij die dit kan overnemen. Dit is om twee redenen belangrijk:

1. Indien een partij IRMA als authenticatiemiddel wil inzetten, moet deze klanten naar de gemeente Nijmegen sturen om de gegevens op te halen. Dit is voor landelijk opererende organisaties een drempel.
2. De tijdelijkheid maakt dat het voor deze partijen onzeker is of de verstrekking in de toekomst plaats blijft vinden.

Hierover is overlegd met het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, de Rijksdienst voor Identiteitsgegevens en Logius. Alle drie deze partijen kunnen de verstrekking via IRMA niet (op korte termijn) overnemen.

Daarnaast vindt de verstrekking momenteel plaats via DigiD, waardoor het betrouwbaarheidsniveau van de gegevens afhankelijk is van het betrouwbaarheidsniveau van DigiD.

Tot slot is het voor gemeenten niet vanzelfsprekend om IRMA in de dienstverlening in te zetten. Momenteel zijn er geen leveranciers die een IRMA authenticatiemogelijkheid aanbieden aan gemeenten.

5. Projectdoelstellingen

De doelstelling van dit project om de drie genoemde problemen; een landelijke verstrekking, verstrekken op hoog betrouwbaarheidsniveau en het gebruik van IRMA voor gemeenten eenvoudiger maken, voor het eind van 2019 op te lossen.

Hiervoor zijn 3 SMART doelstellingen beschreven

1. In het tweede kwartaal van 2019 is het mogelijk om via meerdere gemeenten gegevens uit de BRP verstrekt te krijgen via IRMA in een 'onafhankelijk label'.
2. In het derde kwartaal van 2019 zijn er IRMA API's beschikbaar die gemeenten en andere organisaties kunnen inzetten in de dienstverlening
3. Voor het eind van 2019 is het mogelijk om gegevens uit de BRP verstrekt te krijgen via IRMA op eIDAS betrouwbaarheidsniveau 'hoog'

6. Deelprojecten

Voor de drie doelstellingen worden onafhankelijke deelprojecten opgezet. Dit om de afhankelijkheid tussen de drie doelstellingen te minimaliseren.

6.1 Gezamenlijke gemeentelijke verstrekking

Aangezien het op korte termijn niet mogelijk is om de verstrekkingen uit de BRP via een landelijke partij te organiseren is het aan gemeenten, de beheerders van de BRP, om de gegevens te verstrekken aan inwoners. Het doel van dit deelproject is dan ook om dit beschikbaar te maken voor alle inwoners middels een 'onafhankelijk middel'.

6.1.1 Randvoorwaarden

Om dit mogelijk te maken zijn er een aantal randvoorwaarden waaraan voldaan moet worden vanuit de techniek van de stichting Privacy by Design en de gebruikers.

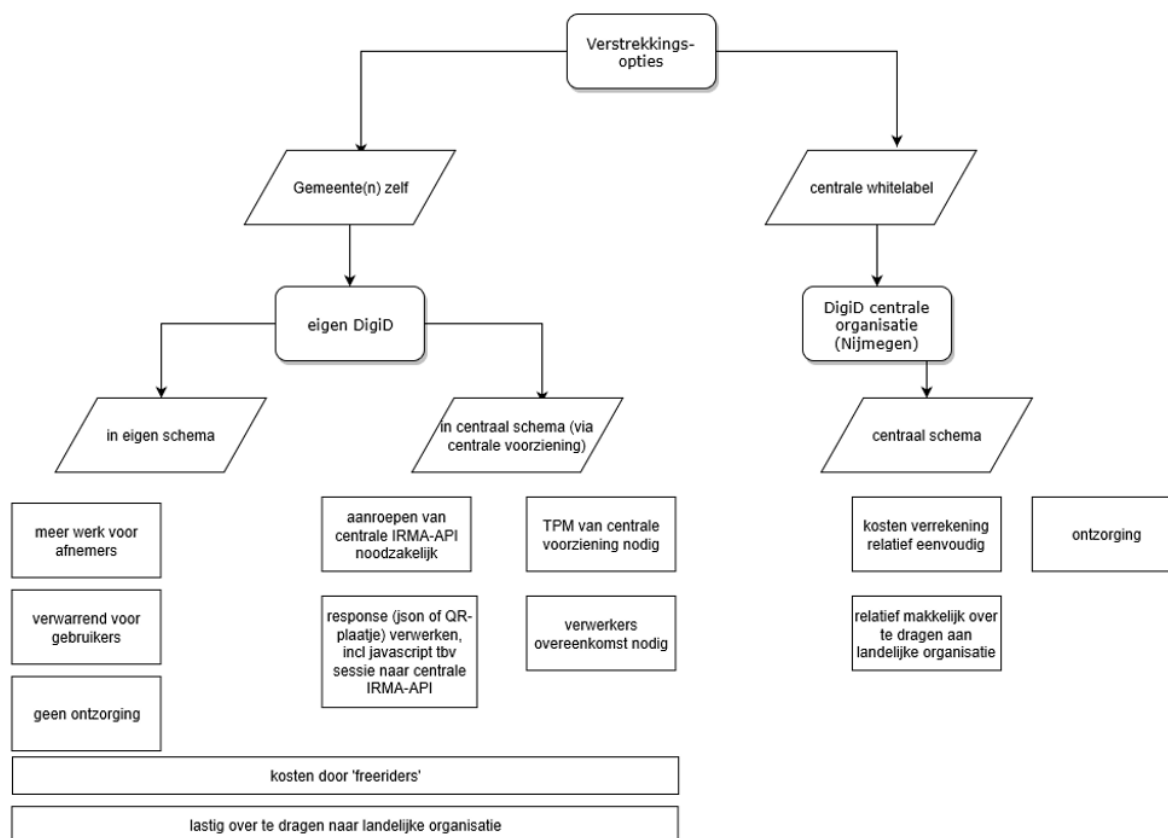
- Het is slechts mogelijk om met 1 private key BRP attributen te verstrekken in het IRMA BRP schema. Hierdoor kan er slechts één 'verstrekkings API' bestaan
- De gegevens worden hierdoor uitgegeven met één naam 'gemeenten' in plaats van 'gemeente A', 'gemeente B' etc.

6.1.2 Vooronderzoek verstrekkingsopties

Er is onderzocht welke opties er zijn voor de verstrekking van attributen op landelijk niveau. Hier kwamen de volgende opties naar voren

- Via één landelijke pagina, gehost door één gemeente of instantie namens alle gemeenten
- Via iedere afzonderlijke gemeente; iedere gemeente heeft een verstrekkingsscherm, welke via de eigen DigiD naar de 'Verstrekkings API' gaat, waarna op de eigen gemeentepagina de verstrekking plaatsvindt

Dit heeft geleid tot onderstaande mogelijkheden:



6.1.3 conclusie vooronderzoek

Op basis van deze bevindingen is ervoor gekozen om de één pagina verstrekking in te gaan richten. De nadelen wat betreft de verwerkersovereenkomsten, de lastig te verdelen kosten en de TPM zijn dusdanig remmend in het proces dat op deze wijze er niet op korte termijn opgeschaald kan worden.

6.1.4 Credentials

De huidige attributen die de gemeente Nijmegen levert zijn ondergebracht in 4 credentials⁹, te weten:

- BSN
- Persoonsgegevens
- Adres
- Leeftijdslimieten

Uit de pilot komt naar voren dat dit fraude in de hand kan werken. Om deze reden worden in het niet wenselijk dat de persoonsgegevens verspreid worden over meerdere credentials. Vandaar dat de volgende credentials met attributen worden voorgesteld:

Persoonsgegevens

BSN

Voorletters

Voornamen

Voorvoegsel

Geslachtsnaam

Achternaam

Volledige naam

Geboortedatum

⁹ Groepjes attributen

Geslacht
Nederlandse nationaliteit
Leeftijdslimieten
DigiD niveau

Adres

Straat
Huisnummer
Postcode
Gemeente
Woonplaats

6.1.5 Roadmap

Actie	Door	Datum
Twee nieuwe credentials maken met 'gemeenten' attributen, waaronder betrouwbaarheidsniveau	Nijmegen / Privacy by Design	Januari 2019
Opleveren nieuw schema	Nijmegen / Privacy by Design	Februari 2019
Whitelabel website maken	Nijmegen	Februari 2019
Live gaan	Nijmegen	Maart 2019

6.2 Verstrekken via zuil

De gemeenten Almere, Leiden en Haarlem hebben tijdens het digitale identiteitslab van BZK, Utrecht en de Waag gewerkt aan een use case waarbij IRMA als tool werd gebruikt. Tijdens deze sessies zijn er verschillende concepten uitgewerkt. één van deze concepten is het ontwikkelen van een IRMA zuil. Met deze zuil kan je informatie die op je paspoort / rijbewijs staat overzetten naar je telefoon. Waarbij een aantal belangrijke attributen worden geladen, waaronder je persoonsgegevens maar ook een gecontroleerde pasfoto. Deze zuil is nodig omdat niet alle smartphones hun NFC chip hebben open gezet voor dit soort toepassingen. Daarnaast is het neerzetten van een zuil in b.v. de publiekshal of bibliotheek nodig om inwoners zonder Digid of die graag begeleid worden in het proces voorwaarde voor digitale inclusie. Het potentieel van een dergelijke zuil is groot, naast je paspoort zou het ook een 'winkel' kunnen zijn voor meer attributen (denk b.v. aan rijvaardigheid,...) maar is ook het eidas niveau hoog theoretisch mogelijk. Om dit niveau überhaupt te kunnen bereiken is een persoonlijke identificatie noodzakelijk. Een host of balie medewerker zou na identificatie van de inwoner de persoonsattributen op niveau hoog kunnen afgeven. De IRMA foundation heeft deze code in concept werkent op de plank liggen. Om dit concept te laten werken is doorontwikkeling van de code, integratie in een zuil en uitgebreide gebruikers testen nodig.

6.3 Gebruik van IRMA

Dit stuk behoeft nog nadere invulling.

7. kosten

Kosten voor dit project zijn op te knippen in 2 soorten. Structurele en variabele kosten.

7.1 Structurele kosten

Om de landelijke verstrekking mogelijk te maken is het noodzakelijk dat er een degelijke infrastructuur staat voor zowel de verstrekking bij de gemeente als goed onderhoud bij de Stichting Privacy by Design.

De kosten voor de gemeente worden geschat op €100.000 per jaar. Deze bestaan uit:

- Serverkosten, het draaiend houden van de API, berichtenverwerking, storage
- Projectkosten voor doorontwikkeling schema, realisatie webpagina', onderhoud GBA koppeling, bugfixing, organisatie landelijke samenwerking

De kosten voor de stichting Privacy by Design worden eveneens geschat op €100.000 per jaar. Deze bestaan uit:

- Doorontwikkeling app, waaronder verbetering van de usability en verbeterde mogelijkheden voor ondertekening.

7.2 Variabele kosten

Per verstrekking worden er kosten gemaakt. Deze kosten bestaan uit €0,14 DigiD kosten en €0,10 GBA-v kosten (prijspeil 2019).

Deze kosten worden per kwartaal gefactureerd aan de VNG. Indien er geen groen licht komt vanuit de VNG zullen de kosten gefactureerd worden aan de betreffende gemeente. Dit zal gebeuren vanaf 20 verstrekkingen per gemeente. Voor de 'kleine afnemers' zullen afspraken met de VNG gemaakt worden.

7.3 overzicht

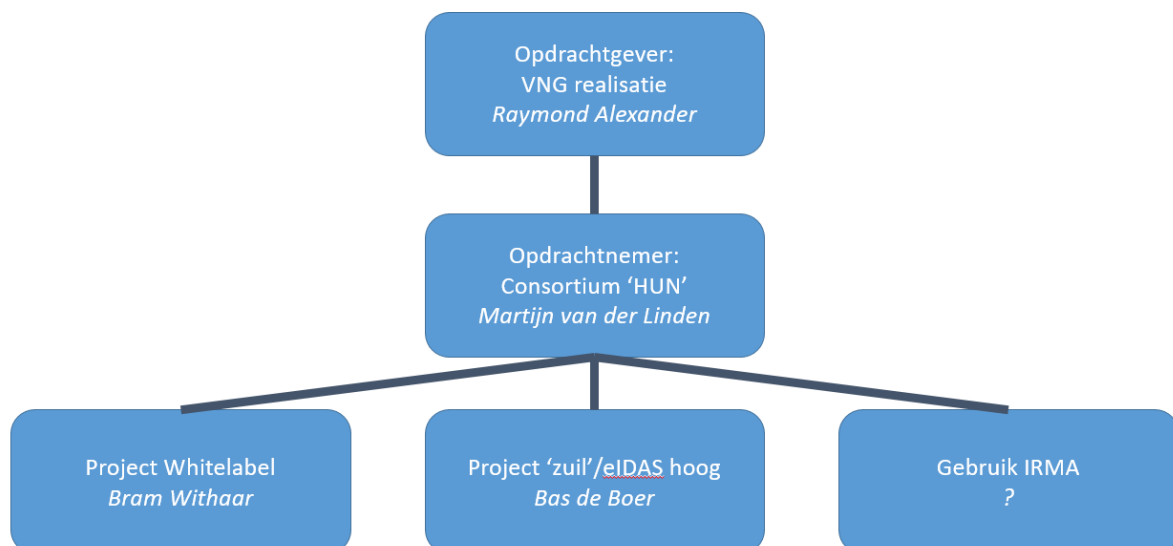
In onderstaande tabel zijn de kosten voor de IRMA verstrekking weergegeven.

Vast	
Kosten beheer + project gemeente Nijmegen	€100.000 per jaar
Kosten beheer Privacy by Design	€100.000 per jaar
Variabel	
Verstrekking	€0,25 per verstrekking

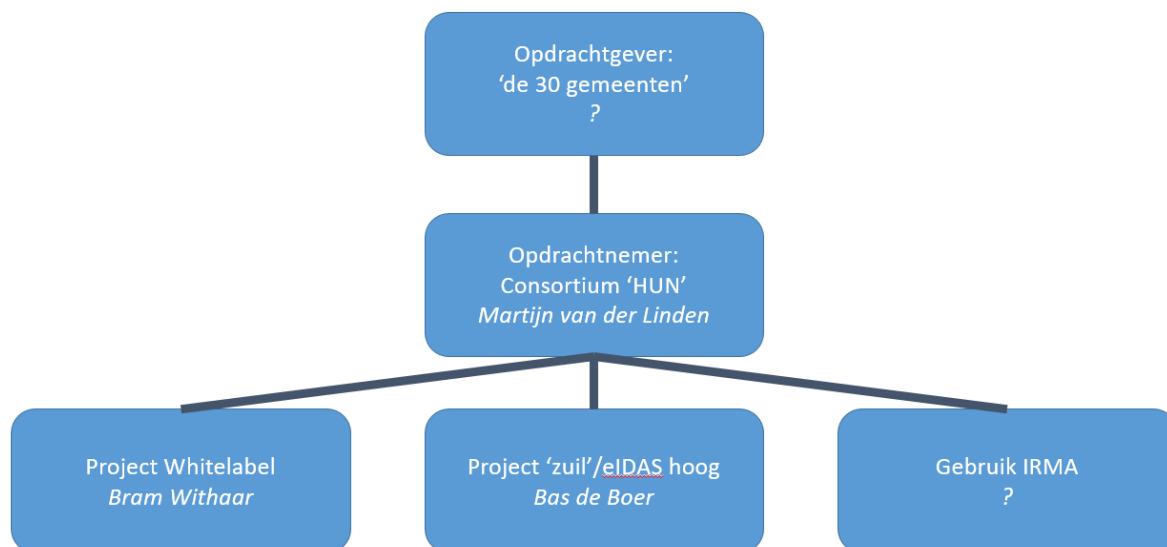
8. Projectorganisatie

Er zijn twee mogelijkheden om dit project te ondersteunen. In den beginnen wordt uitgegaan van opdrachtgeverschap door de VNG. Mocht het programma 'Samen Organiseren' dit project niet omarmen, dan zal optie 2 in beeld komen.

8.1 Optie 1: opdrachtgeverschap vanuit VNG



8.2 Optie 2: opdrachtgeverschap zonder VNG



9. Potentieel Onderschrijvende gemeenten en organisaties

De volgende gemeenten ondersteunen dit voorstel:

Gemeente	Contactpersoon
Alblasserdam (via Drechtsteden)	Dennis van der Valk
Almere	Jan Willem Woolderink / Joël Koeckhoven
Arnhem	Anne Goris
Buren	Holger Peters
Deventer	Paulien Brinkman / Renze Zijlstra
De Bilt	Tom Meeuwesse
Dongen	Julian Wassink
Dordrecht (via Drechtsteden)	Dennis van der Valk
Eindhoven	Dewi Delhoofen
Enschede	Petra Bout
Emmen	Jan Willem Bos
Haarlem	Bas de Boer
Hardinxveld-Giessendam (via Drechtsteden)	Dennis van der Valk
Heerhugowaard	Rob Heimerling
Hendrik-Ido-Ambacht (via Drechtsteden)	Dennis van der Valk
's-Hertogenbosch	Mathieu Rutten
Hollandse Kroon	Marco Brederveld
Meierijstad	Dorothee de Louw / Carl van der Pol
Leiden	Jasmijn Mulder
Lingewaard	Victoria Lamers
Nijmegen	Bram Withaar / Martijn van der Linden
Oldenzaal	Mike Tanke
Oss	Frank van de Leur / Wenny Bruysters
Papendrecht (via Drechtsteden)	Dennis van der Valk
Sliedrecht (via Drechtsteden)	Dennis van der Valk
Tilburg	Brigitta Kop
Utrecht	Donovan Karamat Ali
Zwijndrecht (via Drechtsteden)	Dennis van der Valk

De volgende organisaties ondersteunen dit voorstel potentieel:

Organisatie	Contactpersoon
IMG 100.000+	Cees van Westrenen
Dimpact	Jaap van Vliet
Logius	Leon van der Ree / Jaron Azaria
Ministerie van BZK	Sandra Lentjes / Wouter Welling
Stichting Privacy by Design	Bart Jacobs / Sietse Ringers
VDP	Jan Fraanje
VIAG	Cees van Westrenen
VNG Realisatie	Peter ter Telgte / Raymond Alexander