

Voorstel Digitale Identiteit via IRMA

Voorstel

Aan het GGU-fonds wordt voorgesteld om:

0. IRMA¹ te gebruiken als een 'digitale identiteit' die zowel publiek als privaat gebruikt kan worden voor een periode van, ten minste, 2 jaar.
1. Vanaf maart 2019 gegevens uit de basisregistratie personen beschikbaar te laten stellen via IRMA, zodat gemeenten en private partijen IRMA kunnen gebruiken voor authenticatie.
2. Hiervoor Jaarlijks €200.000 beschikbaar vanuit het GGU-fonds om de structurele kosten te dekken, voor maximaal 2 jaar.
3. De variabele kosten voor het verstrekken van gegevens uit de basisregistratie personen te financieren vanuit het GGU-fonds, voor maximaal 2 jaar

Dit voorstel wordt onderschreven door de gemeenten in bijlage 1

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'². De drie elementen van deze digitale identiteit zijn in 2018 omschreven in een position paper³.

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 WAAG⁴.

In het kader van dit identiteitslab heeft de gemeente Nijmegen een verstrekking uit de basisregistratie personen (BRP) gerealiseerd via IRMA (I Reveal My Attributes)⁵. 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 Nederlandse Privacy Award 2018 van Privacy First, de Brouwerprijs voor Wetenschap en Samenleving⁷ ontvangen en is het door Internet Society Nederland uitgeroepen tot beste internetinnovatie van 2019⁸.

¹ Bijlage 2: Over IRMA (I Reveal My Attributes)

² <https://vng.nl/onderwerpenindex/bestuur/brieven/alv-voorstel-gezamenlijke-gemeentelijke-uitvoering-2019>

³ <https://vng.nl/onderwerpenindex/dienstverlening-en-informatiebeleid/dienstverlening-aan-inwoners-en-ondernemers/nieuws/vng-position-paper-digitale-identiteit>

⁴ <https://digitaleidentiteit.waag.org/>

⁵ <https://tweakers.net/nieuws/143823/nijmegen-test-identificatieapp-irma-die-privacy-waarborgt.html>

⁶ Zie voor de gehele voorgeschiedenis bijlage 3

⁷ <https://www.khmw.nl/privacy-by-design-ontvangt-brouwer-prijs-2018/>

⁸ <https://awards.isoc.nl/innovatie/2019/>

2. Doel van het voorstel

Het doel van dit voorstel is om de inwoners van Nederland een ‘digitale identiteit’ te bieden die voldoet aan de voorwaarden zoals gesteld in de position paper.

Met deze digitale identiteit kan de inwoner zich identificeren, authenticeren of autoriseren in zowel het publieke als het private domein. Hier is een grote maatschappelijke behoefte aan en er is momenteel nog geen andere oplossing voor dan IRMA. Aangezien ‘de gemeenten’ de enige partij is die deze oplossing handen en voeten kan geven, wordt aan het GGU-fonds gevraagd om deze oplossing financieel te ondersteunen.

2.1 subdoelen

Naast dit hoofddoel onderschrijft dit voorstel tevens drie subdoelen:

1. Het verstrekken van gegevens op eIDAS niveau hoog
2. Het toepassen van IRMA in de gemeentelijke dienstverlening
3. Gebruik identificatie op processen waar geen BSN is toegestaan

Subdoel 1 is relevant aangezien er in verschillende domeinen, waaronder het zorgdomein, gewerkt moet worden met bijzondere persoonsgegevens. Deze mogen alleen met het hoogste betrouwbaarheidsniveau uitgewisseld worden. Om de door de gemeenten ondersteunde toepassing op alle kanalen toepasbaar te laten zijn, is het noodzakelijk dat eIDAS niveau hoog behaald wordt.

Subdoel 2 is relevant aangezien een ‘digitale identiteit’ slechts iets is, als het daadwerkelijk bruikbaar is. Gemeenten kunnen hierin een belangrijke rol spelen. Daarnaast zijn gemeenten momenteel afhankelijk van DigiD, om 24uursdienstverlening is het wenselijk dat er een tweede veilige inlogmethode is voor het geval dat er een storing is binnen DigiD.

Subdoel 3: Binnen gemeentelijke overheden zijn er tal van (digitale) processen waarbij het gebruik van een BSN niet is toegestaan, maar waar een vorm van authenticatie wel wenselijk is. Denk hierbij aan privaatrechtelijke handelingen als het verhuur van sportaccommodaties of de verkoop van gronden. Momenteel is hier geen betrouwbare digitale vorm van authenticatie mogelijk. IRMA kan hier mogelijk een uitkomst voor bieden.

3. Digitale identiteitsmiddelen

Momenteel zijn er diverse middelen die prefereren de nieuwe digitale identiteit te zijn. In bijlage 4 zijn deze middelen technisch en functioneel omschreven. In onderstaande tabel is een samenvatting gemaakt van de resultaten van de inventarisatie.

Eigenschap	iDIN	SSI	vID	Me	Itsme	Qiy	IRMA
Fase	Productie	Prototype	Testfase	Gestopt	Productie in België	‘afspraken stelsel’	Productie
Online	+	+	+	+	+	+	+
Offline							+
OpenSource		+				+	+
Privacy by design		+	+	+		+	+
Juridisch akkoord NL/EU	+		+			+	+
Privacy Assessment						+	+
Multiplatform		+		+	+	+	+
Gebruiksvriendelijkheid	+	+			+	+	+
Gratis gebruik	+	+		+	+	+	+
Regie op gegevens							+

Uit deze inventarisatie blijkt dat IRMA op dit moment het middel is dat voldoet aan alle eisen die worden aan een digitale identiteit. Uiteraard hebben andere oplossingen SSI of nog onbekendere buitenlandse middelen de mogelijkheid om ook aan alle eisen te voldoen. Echter gezien de huidige behoefte is het wenselijk om vanaf nu een oplossing ter beschikking te stellen aan gemeenten en private partijen.

4. Projectonderdelen

Het project bestaat uit de volgende onderdelen:

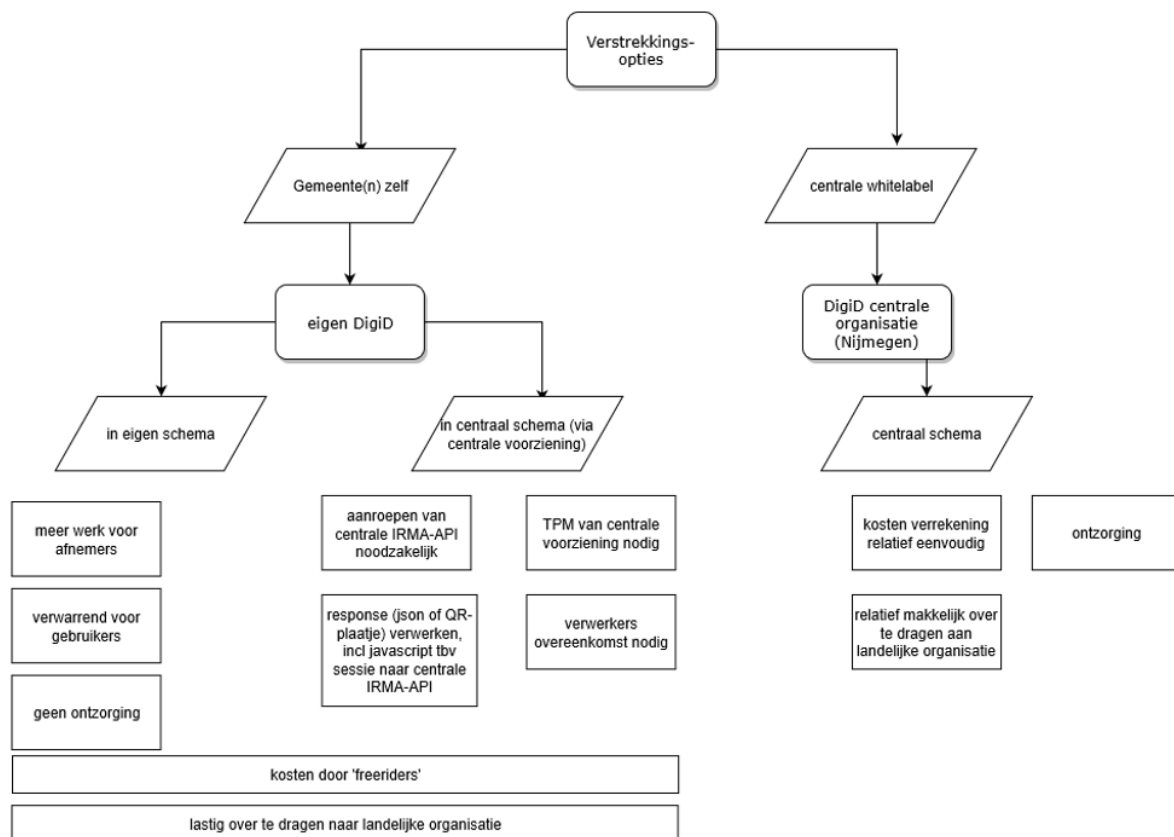
1. Het landelijk verstrekken van attributen uit de BRP
2. Het maken van een procedure die kan leiden tot een hoger eIDAS niveau / voor niet digitaal vaardigen
3. Pilots in de praktijk

4.1 Landelijk verstrekken

Er is onderzoek gedaan naar de meest haalbare weg voor het verstrekken van BRP attributen. Hier is gekeken naar 2 opties:

1. Het verstrekken van gegevens door via gemeenten
 - a. Via eigen verstrekking
 - b. Via centrale verstrekking
2. Een centrale verstrekking via één gemeente

Dit heeft geleid tot onderstaand schema:



Hieruit blijkt dat de meest haalbare optie het verstrekken via een centrale verstrekkingsovereenkomst is. De gemeente Nijmegen heeft een dergelijke voorziening reeds draaien. Het voorstel voorziet dan ook een centrale voorziening via een 'blanco' service beheert door de gemeente Nijmegen.

4.1.1 verstrekte attributen

De volgende attributen worden verstrekt aan de inwoner:

Persoonsgegevens	Adres
BSN	Straat
Voorletters	Huisnummer
Voornamen	Postcode
Voorvoegsels	Gemeente
Geslachtsnaam	Woonplaats
Achternaam	
Volledige naam	
Geboortedatum	
Geslacht	
Nederlandse Nationaliteit	
Leeftijdslimieten	
DigiD niveau	

Met deze attributen kunnen inwoners de belangrijkste zaken regelen. Er is bewust gekozen om geen gegevens van ouders en kinderen te verstrekken, aangezien in de BRP niet aangetoond kan worden of een ouder het wettelijk gezag heeft over een kind. Ook worden afgeleide gegevens als de verblijfstitel en gegevens van reisdocumenten niet uitgegeven.

4.2 eIDAS niveau / digitale inclusie

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 werkend op de plank liggen. Om dit concept te laten werken is doorontwikkeling van de code, integratie in een zuil en uitgebreide gebruikers testen nodig.

4.3 Pilots in de praktijk

Om IRMA ook in de praktijk toe te passen zijn er bij diverse gemeenten en instellingen plannen om pilots te starten. Voorbeelden hiervan zijn:

- Pre-fill van webformulieren
- Alternatieve authenticatie naast DigiD
- Leeftijdscheck bij horecagelegenheden
- Uitwisselen van inkomstgegevens
- Telefonische authenticatie

Om deze pilots op elkaar te laten aansluiten zal er eind maart / begin april een bijeenkomst worden georganiseerd om hier lijn in aan te brengen. Van hieruit zal een community worden gebouwd waarin IRMA initiatieven worden uitgewisseld en gedeeld onder gemeenten.

4.4 Roadmap

Uit eerder genoemde pilots komt de volgende roadmap

Tijdspad	Onderdeel	Frequentie
Maart 2019 – april 2021	Verstrekking BRP attributen	Continu
April 2019 – april 2021	Community IRMA pilots	2 maandelijks
April 2019 – april 2021	Overleg BZK, Logius, RvIG over overdracht	Maandelijks
Mei 2019 – april 2021	Procedure zuil / balieproces	Continu

5. Financiële onderbouwing

De aanvraag ziet toe op twee financiële componenten: een structurele bijdrage van €200.000 per jaar voor zolang gemeenten BRP attributen verstrekken en de variabele kosten van ██████ per verstrekking.

5.1 Structurele kosten

WOB art. 10 lid 2 b

[illegible]

5.2 Variabele kosten

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

Het voorstel is om de kosten per kwartaal te factureren bij het GGU-fonds. In een openbare rapportage zal bijgehouden worden vanuit welke gemeente de verstrekkingen plaatsvinden.

Bijlage 1: Onderschrijvende gemeenten

Alblasserdam

Alkmaar

Almere

Amersfoort

Amsterdam

Arnhem

Boekel

Breda

Bureau Drechtsteden

Buren

De Bilt

Deventer

Dienstverlening Drechtsteden

Dordrecht

Eindhoven

Emmen

Enschede

Gemeentelijke Belastingdienst Drechtsteden

Groningen

Haarlemmermeer

Hardinxveld-Giessendam

Heerenveen

Helmond

Hendrik-Ido-Ambacht

ICT Rijk van Nijmegen

Meierijstad

Nijmegen

Onderzoekscentrum Drechtsteden

Oss

Papendrecht

Servicecentrum Drechtsteden

's-Hertogenbosch

Sliedrecht

Sociale Dienst Drechtsteden

Súdwest-Fryslân

Utrecht

Utrecht

VDP

Zwijndrecht

Bijlage 2: Over IRMA

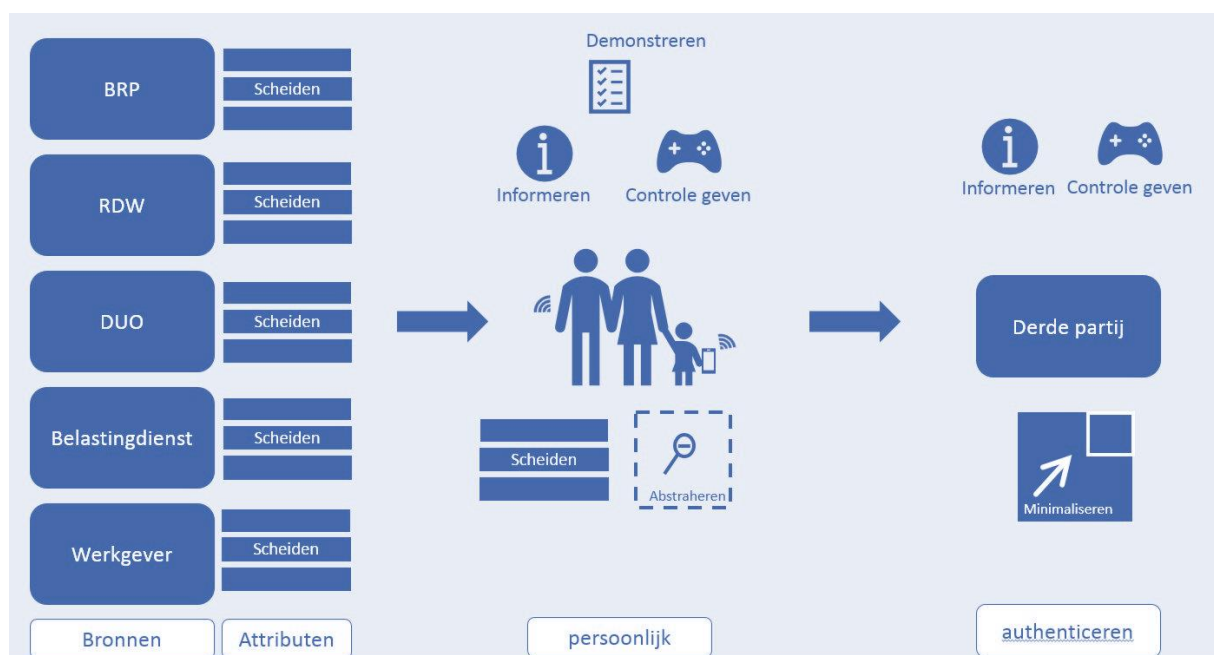
IRMA, *I Reveal My Attributes*, is een privacy vriendelijk identiteitsplatform voor zowel authenticatie als ondertekening⁹. Dit staat vermeld op de site van de Privacy by Design Foundation, die zicht richt op de ontwikkeling en het gebruik van IRMA.

1. Stichting Privacy by Design

De stichting en het platform zijn ontstaan vanuit de onderzoeksgroep '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 persoonsgegevens, wordt het al een stukje minder privacygevoelig. 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. Attribuut gebaseerde identiteit

De IRMA omgeving maakt het mogelijk om vanuit bestaande registraties, zoals de BRP¹⁰ 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 hoef 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).

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

¹⁰ Basisregistratie personen

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

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'.

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.

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. IRMA is uit deze situatie aan het ontsnappen en krijgt tractie in verschillende sectoren.

Bijlage 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.

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.

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.

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.

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.

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. 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. Landelijke verstrekking

Om IRMA in beschikbaar te maken voor landelijke partijen, is het wenselijk dat deze niet via 'de gemeente Nijmegen' verstrekt worden. Hiervoor zijn gesprekken gevoerd met de RvIG, Logius en het Ministerie van Binnenlandse zaken. Hieruit bleek dat het om hen moverende redenen niet mogelijk is om op korte termijn over te gaan op verstrekkingen van BRP gegevens middels IRMA.

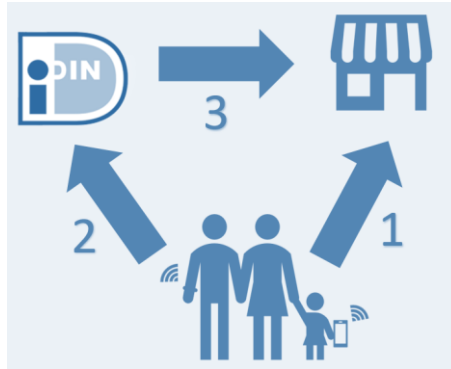
Daardoor is overgeschakeld op de 'gemeentelijke route'. Zoals in de wet beschreven is het verstrekken van gegevens een gemeentelijke taak. Hiervoor is op 5 februari een bijeenkomst georganiseerd voor gemeenten. De gemeenten die aanwezig waren bij deze bijeenkomst staan achter het plan om over te gaan op een landelijke gemeentelijke verstrekking.

Bijlage 4: analyse middelen digitale identiteit

1. iDIN

iDIN¹¹ is de digitale identiteit die de banken in 2017 hebben geïntroduceerd. Een site kan de iDIN inlogmethodiek voor de site zetten, waarna de inwoner via zijn of haar bank inlogt op de website. De site ontvangt dan de gegevens zoals vastgelegd bij de bank.

Schematisch ziet dit er als volgt uit:



figuur 1: inloggen met iDIN

Het voordeel van deze systematiek is dat de inwoner de wijze herkent vanuit de iDEAL betaling. Echter, de site ontvangt de gegevens via de bank. De bank krijgt hierdoor inzage in het surfgedrag van de inwoner. Ook moet de site vertrouwen op de gegevens die de bank van een inwoner heeft. Deze kan in redelijke mate worden vertrouwd, echter het gegeven 'adres' is voor de meeste bankzaken niet relevant en het gegeven 'BSN' mag door een bank ook niet gebruikt worden.

Om iDIN te gebruiken heeft een site een contract nodig met een bank. Deze vraagt tussen de €0,25 en €0,40 per inlog middels dit systeem. iDIN heeft momenteel geen plannen om het uit te bereiden en beschikbaar maken voor ondertekening en gebruik buiten internet.

2. SSI

SSI, Self Sovereign Identity, is een project dat loopt bij de rijksdienst voor identiteitsgegevens in samenwerking met de TU Delft en IDEMIA, het bedrijf dat verantwoordelijk is voor de productie van paspoorten. Hierbij wordt middels de Blockchainvariant 'Trustchain' met een app op de telefoon de chip van het paspoort of de identiteitskaart uitgelezen. Door het maken van een Selfie wordt de foto op het document vergeleken met de houder van de telefoon en de gegevens van het paspoort kunnen vervolgens digitaal gebruikt worden.

Dit project bevindt zich in de prototyping fase. Momenteel wordt een projectleider geworven¹² om het komende jaar dit prototype verder uit te werken, de juridische gevolgen te onderzoeken en het prototype te testen.

3. vID

Een project van de rijksdienst voor identiteitsgegevens dat al verder is het virtueel ID. Hierbij worden eveneens met een app de gegevens van de chip van de identiteitskaart of het paspoort uitgelezen en opgeslagen in de app. Deze gegevens kunnen vervolgens middels een door de app te genereren QR code gebruikt worden door een andere partij.

Hieraan kleven 2 nadelen: alleen de gegevens vanuit het document kunnen gebruikt worden en Apple staat niet toe dat de vID app de chip van een paspoort uitleest. Hierdoor kan de app vooralsnog alleen gebruikt worden op een android telefoon.

¹¹ <https://www.idin.nl/>

¹² <https://zp-en-co.nl/vacature/a-20190365-projectleider-ssi/>

De rijksdienst voor identiteitsgegevens heeft formeel nog niets gepubliceerd over dit project. Er is ook geen datum bekend wanneer de app gelanceerd wordt.

4. Me app

Stichting Forus¹³ heeft op basis van het blockchainplatform 'Ethereum' de digitale identiteitsapp 'Me'¹⁴ ontwikkeld. Deze app wordt momenteel gebruikt om 'het kindpakket' op te draaien, waarin leveranciers en inwoners krediet kunnen uitwisselen in het kader van minimaregelingen. Een extra functionaliteit is het opbouwen van een 'profiel' dat ingezet kan worden voor andere toepassingen.

Tijdens het identiteitslab is deze oplossing getest met de case over decentrale democratie. Hieruit is gebleken dat het platform van Forus zeer geschikt is voor processen, maar de 'identiteit' te beperkt is om in te zetten als 'digitale identiteit', aangezien de techniek hier nog niet geschikt voor is.

Stichting Forus heeft zelf aangegeven zich niet meer te gaan richten op de digitale identiteit. De focus zal liggen op de doorontwikkeling van het platform voor (minima)regelingen.

5. Itsme

Itsme¹⁵ is een in België ontwikkelde identiteitsapp die werkt met behulp van je simkaart op de telefoon¹⁶. Via de kaartreader zoals deze in België wordt gebruikt worden de gegevens van je Identiteitskaart uitgelezen en opgeslagen op een centrale server van Itsme. De gegevens worden in de app getoond door middel van het ingeven van een 5-cijferige pincode welke is opgeslagen op de simkaart. Via de app kunnen gegevens verstrekt worden aan een derde partij. De uitwisseling gebeurt via een beveiligd 3g en 4g netwerk.

Schematisch ziet dit er als volgt uit:



figuur 2: inloggen met itsme

Binnen Itsme worden alleen gegevens opgeslagen die afkomstig zijn vanuit de identiteitskaart en van de bank. Itsme wordt ontwikkeld en beheerd door Belgian Mobile ID¹⁷, een consortium van 7 banken en telecomproviders.

6. Qiy

In 2015 heeft de Qiy foundation het afsprakenstelsel Qiy¹⁸ ontwikkeld. Op basis van een afsprakenstelsel kunnen persoonsgegevens worden uitgewisseld voor het gebruik maken van diensten. De inwoner geeft toestemming dat partijen binnen het afsprakenstelsel gegevens uitwisselen over deze inwoner.

¹³ <https://forus.io/>

¹⁴ <https://forus.io/me-app>

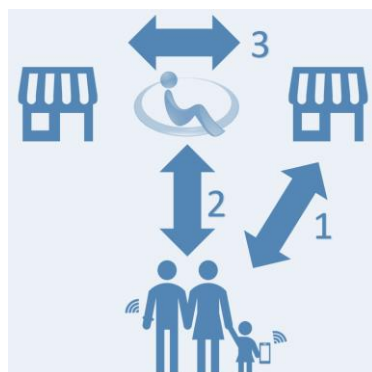
¹⁵ <https://www.itsme.be/>

¹⁶ In de Nederlandse versie wil men deze koers loslaten

¹⁷ <https://www.belgianmobileid.be/nl>

¹⁸ <https://www.qiyfoundation.org/>

Schematisch ziet dit er als volgt uit:



Figuur 3: het Qiy afsprakenstelsel

In tot en met 2017 zijn diverse tests gedaan met het Qiy afsprakenstelsel¹⁹ en in 2016 heeft het forum standaardisatie een rapport gemaakt over de toepasbaarheid van dit stelsel²⁰. Echter, geen van deze tests is omgezet naar een concreet project. Wel is de documentatie over Qiy in 2018 op Github gezet.

7. IRMA

IRMA is ontstaan uit de onderzoeksgroep 'digital security' van de Radboud Universiteit²¹. Sinds 2008 is onderzoek gedaan naar een attribuut gebaseerde identiteit. Nadat het onderzoek was afgerond is in 2016 de Stichting Privacy by Design²² opgericht om het onderzoek in de praktijk te brengen en de IRMA technologie verder te professionaliseren.

Binnen het IRMA ecosysteem moet de inwoner eerst de gegevens ophalen bij een 'verstrekker'. De gegevens worden vervolgens opgeslagen binnen de app op de mobiele telefoon. De app is beveiligd met een PINcode bestaande uit minstens 5 cijfers. Vervolgens kan de gebruiker de gegevens inzetten om zich te autoriseren, in te loggen of te identificeren bij een derde partij.

Voordat gegevens verstrekt of opgehaald kunnen worden, moet een sessie worden vrijgegeven. Dit kan door een pincode in te voeren, waarna vervolgens een ander deel van de sleutel wordt vrijgegeven door de Stichting Privacy by Design.

Schematisch ziet dit er als volgt uit:

¹⁹ https://depilotstarter.vng.nl/sites/default/files/project_bestand/151105_impactanalyseqiy_definitief.pdf

²⁰

https://www.forumstandaardisatie.nl/sites/bfs/files/proceedings/FS%20161019.9A%20Rapport%20van%20bevindingen%20Qiy%201.3_0.pdf

²¹ <https://www.ru.nl/ds/>

²² <https://privacybydesign.foundation/>



figuur 4: Het IRMA ecosysteem

IRMA is voor webshops en andere partijen gratis te gebruiken. De software is open source en is te vinden op Github²³. Om als partij gegevens via IRMA te verstrekken, moeten deze gegevens worden toegevoegd aan het verstrekkingsschema²⁴. Hiervoor is medewerking nodig van de Stichting Privacy by Design.

Momenteel bevat IRMA; gegevens uit de basisregistratie personen, geleverd door de gemeente Nijmegen; de AGB code, geleverd door stichting NUTS en diverse andere gegevens geleverd door de stichting zelf, waaronder iDIN, BIG en diploma gegevens, telefoonnummer en e-mail.

²³ <https://github.com/privacybydesign>

²⁴ <https://github.com/privacybydesign/pbdf-schememanager>