Whitepaper

Naar een inlogstelsel voor de informatiesamenleving

Kies nu de juiste scope en doelstelling voor het eID programma

Door: Dirk Schravendeel

PBLQ
verbinders in de informatiesamenleving

Om succesvol te zijn is een koerswijziging van het eID programma nodig. We stellen voor om daarvoor terug te grijpen op het ontwerp van het eID stelsel dat in 2014 is opgesteld. Het is urgent om nu een aangepaste scope en doelstelling te kiezen om het programma succesvol te kunnen uitvoeren. In dit whitepaper vragen we daar aandacht voor en geven we aan hoe we tot de bovenstaande conclusie zijn gekomen. De redenering start bij de behoeften van "Sara", een deelneemster in de informatiesamenleving.
Na een schets van de problemen die aan het ontstaan zijn binnen de huidige scope van het programma geven we aan hoe deze vermeden kunnen worden. De extra kansen die dan ontstaan illustreren we aan de hand van het voorbeeld van het programma Regie op Gegevens.

Samenvatting

Recent stuurde staatssecretaris Knops de herijkte businesscase "Inloggen in het BSN domein. Kosten en baten van het eID stelsel" naar de Tweede Kamer. Die heeft daar ook (op 9 maart) al over gesproken.
Grosso modo is de uitkomst dat de koers van het programma niet zal worden aangepast, maar dat wel scherper gestuurd gaat worden op de kosten.

Uit de businesscase wordt duidelijk dat de scope van wat onder het "eID stelsel" wordt verstaan in de loop van vier jaar aanzienlijk gewijzigd is. Werd daar in 2014 nog een inlogstelsel met drie functionaliteiten (identiteit bekend maken, bevoegdheden bekend maken, gegevens bekend maken) voor de informatiesamenleving onder verstaan[1], nu is de scope versmald tot het beschikbaar maken van middelen om de identiteit bekend te maken in het BSN domein. De bruikbaarheid van de middelen wordt beperkt door verkokering die in de informatiesamenleving helemaal niet voorkomt: scheidingen tussen burger en bedrijfsdomein en even zo tussen publiek en privaat domein.

In de leefwereld van mensen zijn die domeinen één verweven geheel. Het risico bestaat dat de middelen wel gerealiseerd worden, maar zo gebruiksonvriendelijk worden gevonden dat het gebruik ervan maar zeer beperkt zal zijn. Daarnaast ontbreken er dan nog belangrijke functies, zoals machtigingsvoorzieningen en aparte attribuutverklaringen om bij het inloggen bevoegdheden aan te geven en op maat gegevens te verstrekken. En er worden kansen gemist, want een breder inlogstelsel kan ook veel betekenen voor het Gegevenslandschap digitale overheid[2] en het programma Regie op Gegevens[3] dat de grip van burgers op het gebruik wil versterken en ze in staat wil stellen zelf overheidsgegevens te verstrekken.

We beschouwen de korte termijn doelstellingen van het programma als een gegeven. Om voor de langere termijn de doorontwikkeling naar een inlogstelsel met meer functionaliteit als mogelijkheid open te houden, moet op korte termijn besloten worden tot een aanpassing van de scope en de doelstellingen. Dat heeft meteen effect op het ontwerp van de routeringsvoorziening dat nu wordt opgesteld, op de doorontwikkeling van machtigingsvoorzieningen en op besluiten over eHerkenning. Het is echter noodzakelijk om inloggen in de informatiemaatschappij vanuit de overheid adequaat te ondersteunen.

Een deelneemster in de informatiesamenleving: Sara

In ´Identificatie en authenticatie in zorg en ondersteuning´[4] voert VWS onder meer de persona Sara ten tonele. Het verhaal illustreert hoe de informatie-samenleving in de praktijk werkt en welke eisen gesteld moeten worden aan identificatie- en authenticatievoorzieningen.

Sara is 22 jaar en studeerde tot een jaar geleden psychologie aan de Universiteit Utrecht. Na een avondje stappen werd ze aangereden door een stadsbus die geen voorrang gaf. Ze heeft daarbij een dwarslaesie opgelopen. Na een periode van revalidatie pakt ze haar leven weer op. In haar oude studentenkamer op driehoog kan ze niet meer wonen, ze vraagt en krijgt een urgentieverklaring van de gemeente voor een aanpasbare woning. Om zelfstandig te kunnen functioneren moet ze veel regelen om de benodigde hulp en zorg te krijgen. Ze wordt behandeld door meerdere zorgverleners en ze heeft een PGB waarmee ze taxivervoer en een ondersteuner betaalt.

In de informatiesamenleving die nu aan het ontstaan is kan Sara gelukkig veel zaken digitaal regelen. Met haar behandelaren houdt ze haar medische gegevens bij in haar ‘persoonlijke gezondheidsomgeving’ (PGO), waarbinnen zij haar behandelaren toegang geeft tot specifieke onderdelen (autorisatie). Onderlinge afspraken met haar zorgverleners staan in het ‘individueel zorgplan’ (IZP). En in een administratieve module houdt ze haar uitgaven uit haar ‘persoonsgebonden budget’ (PGB) bij, met een koppeling naar de SVB-administratie. Zo kan ze de declaraties van het taxibedrijf direct gebruiken in de verantwoording naar de SVB.

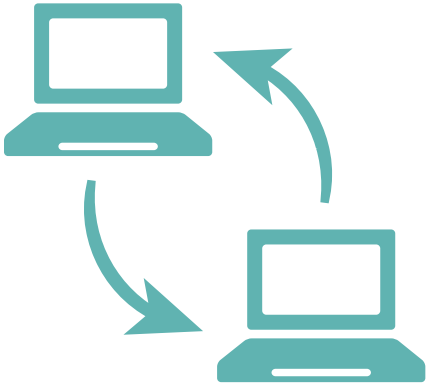
Eisen aan de informatievoorziening

Om Sara in staat te stellen al deze activiteiten uit te voeren moeten de voorzieningen in de informatiesamenleving wel aan een aantal eisen voldoen, onder meer gaat het om de volgende zaken:

- Het betrouwbaar kunnen vaststellen van de identiteit van Sara, zodat ze zich bekend kan maken bij allerlei diensten;
- Het kunnen verlenen van machtigingen door Sara aan een zorgverlener (niet-natuurlijk persoon) of haar vriend (natuurlijk persoon), zodat zij zaken voor haar kunnen regelen;
- De mogelijkheid voor betrouwbare gegevensuitwisseling op een privacybeschermende wijze, zowel in het publieke als in het private domein.

Onderscheid publiek – privaat domein en burger – bedrijf

Opvallend in deze beschrijving van het dagelijks leven van Sara is dat het het persoonlijke, het commerciële en het overheidsdomein continu door elkaar lopen. In de informatiesamenleving is er geen scheiding tussen het private en het publieke domein. Ze heeft te maken met de SVB en het CAK (publiek), zorgverleners en de woningcorporaties (publiek/privaat) en met het taxibedrijf (privaat). Ook de scheiding tussen burger en bedrijf is niet scherp. Wanneer Sara in de toekomst besluit ZZP’er te worden en nog weinig activiteiten onderneemt, kan het gebeuren dat de Belastingdienst haar beschouwt als burger, terwijl ze een subsidieaanvraag bij de RVO als bedrijf moet doen.



“De roldiversiteit die we als persoon dagelijks hebben wordt in de digitale wereld maar beperkt ondersteunt, waardoor we voortdurend tegen systeemgrenzen aanlopen. In de fysieke wereld zijn die grenzen er veel minder.”

Binnen de Digitale Overheid speelt het onderscheid burger – bedrijf en publiek – privaat een grote rol. Dat leidt tot beperkingen van de bruikbaarheid van de gerealiseerde middelen. De overheid werkt aan digitale identificatiemiddelen (DigiD substantieel en hoog) die alleen in het publieke domein en alleen voor de burgerrol gebruikt zullen mogen worden. Machtigingsvoorzieningen en MijnOverheid hebben eveneens een aparte verschijningsvorm voor burgers en voor bedrijven.

De roldiversiteit die we als persoon dagelijks hebben wordt in de digitale wereld maar beperkt ondersteunt, waardoor we voortdurend tegen systeemgrenzen aanlopen. In de fysieke wereld zijn die grenzen er veel minder. De Nederlandse identiteitsdocumenten worden gebruikt in het publieke en private domein. Je mag je dus in de fysieke wereld wel bij een bedrijf identificeren met een overheidsmiddel, maar in de digitale wereld niet. En een bestuurder van een onderneming heeft een apart bedrijfsmiddel, een eHerkenningsmiddel, nodig om zich bij de Kamer van Koophandel bekend te maken.

Het gevolg is dat burgers meerdere middelen voor verschillende domeinen moeten aanschaffen. In de zorgsector wordt het gebruik van persoonlijke gezondheidsomgevingen gestimuleerd. In het programma MedMij is geconstateerd[5] dat mensen voor hun PGO twee authenticatiemiddelen zullen moeten gebruiken: een privaat middel om in te loggen in hun eigen PGO en een publiek middel in de communicatie met zorgverleners.
De reden voor het onderscheid is gelegen in de regels die gelden voor het gebruik van het BSN. In de private sector is gebruik verboden, bij het uitwisselen van zorggegevens is het verplicht. In een impactanalyse die VNG Realisatie heeft uitgevoerd op een pilot met regie op gegevens in de gemeente Boxtel[6] komt een vergelijkbaar probleem aan het licht dat ook met het gebruik van het BSN bij identificatie samenhangt.

Een gevolg kan zijn dat een gebruiker die een aantal transacties doet die voor hem logisch bij elkaar horen, meerdere keren moet inloggen met verschillende middelen. Dat kan zich voordoen in het burgerdomein, maar ook in het bedrijvendomein.

Om bij het Handelsregister een jaarrekening te deponeren moet een bedrijfsmiddel gebruikt worden. Wanneer de ´ultimate benificial owner (UBO)´, die op grond van eigendom en zeggenschap als uiteindelijk belanghebbende is aangemerkt, de jaarrekening heeft gedeponeerd en vervolgens zijn gegevens als UBO wil beheren, kan dat niet met hetzelfde middel. Hij zal moeten uitloggen en weer met een burgermiddel moeten inloggen.

Dit heeft een sterk negatief effect op de gebruikersvriendelijkheid van de identificatiemiddelen van de overheid. Het risico bestaat dat burgers en bedrijven gaan zoeken naar andere middelen die deze beperkingen niet kennen. En als dergelijke middelen er niet zijn, wordt de ontwikkeling van de informatiesamenleving, inclusief de digitale overheid door de gebruiksproblemen geremd.

Een onsje minder met de regels?

Dat onderscheid gemaakt wordt tussen middelen voor publiek of privaat gebruik en tussen burger en bedrijfsrollen heeft deels bestuurlijk-organisatorische redenen: het ministerie van Binnenlandse Zaken en Koninkrijkrelaties was tot voor kort verantwoordelijk voor het beleid ten aanzien van burgers en het ministerie van Economische Zaken en Klimaat (EZK) voor bedrijven. Het wettelijk (in de Wet algemene bepalingen burgerservicenummer) vastgelegde uitgangspunt dat het BSN alleen in het publieke domein gebruikt mag worden, leidt in de praktijk die nu ontstaat tot het onderscheid in middelen voor publiek of privaat gebruik. Dat het BSN alleen voor publiek gebruik beschikbaar is, heeft zijn achtergrond in de regelgeving rond de bescherming van persoonsgegevens. Er wordt wel eens gesuggereerd dat het maar een onsje minder zou moeten met de regels. Dat lijkt ons geen goed idee en het is ook niet nodig, want er zijn andere oplossingen.

Het BSN is ontwikkeld door het programma ‘Stroomlijning basisgegevens’, dat zich tussen 2000 en 2002 richtte op het tot stand brengen van een samenhangende gegevenshuishouding voor de overheid, door de introductie van een stelsel van basisregistraties. Bij de ontwikkeling van het stelsel was een uitgangspunt dat objecten (personen, bedrijven, gebouwen et cetera) in een basisregistratie met een eenduidig uniek nummer geïdentificeerd dienden te worden, zodat elektronische communicatie tussen de basisregistraties onderling, met de dienstverleners en door de dienstverleners onderling, op een eenduidige identificatie van de objecten gebaseerd zou kunnen worden. Anders gezegd: het BSN was nodig om langs de digitale weg bestanden te kunnen koppelen. Dat is de kracht van het nummer, maar vanuit de optiek van de bescherming van persoonsgegevens meteen ook het risico. Destijds is de afweging gemaakt dat het risico binnen het publieke domein voldoende beheersbaar gemaakt kon worden en is het gebruik tot dat domein beperkt.

Sinds het begin van deze eeuw heeft het internet zich enorm ontwikkeld en hebben we in het private domein de opkomst gezien van techgiganten als Google, Apple, Facebook en anderen. Bepaald geen veilige, goed gereguleerde omgeving waarin passende waarborgen geschapen kunnen worden voor het gebruik van een uniek en zeer krachtig identificerend persoonsnummer als het BSN. Er is dan ook geen enkele reden om te veronderstellen dat de afweging nu wel anders kan uitvallen, dat het verantwoord kan zijn om het BSN ook voor gebruik in het private domein beschikbaar te stellen. En wie denkt dat de regels voor de bescherming van persoonsgegevens wel erg strikt zijn en dat daar soepel mee omgegaan zou moeten worden, heeft de Algemene Verordening Gegevens-bescherming niet begrepen. Die geeft het krachtige signaal af dat de regels, die op hoofdlijnen al vijftien jaar van kracht zijn, serieus genomen en aantoonbaar nageleefd dienen te worden.

Bouwstenen van de overheid voor de informatiesamenleving

De overheid is er niet alleen voor zichzelf, maar ook (vooral) ten dienste van de samenleving. De informatiesamenleving is een zeer complex geheel waarin burgers, bedrijven en overheid veel rollen vervullen, zeer verschillende doelen nastreven en met gebruikmaking van een grote diversiteit aan technische middelen met elkaar interacteren. Dat is waar, maar niet nieuw: daarin verschilt de informatiesamenleving niet met de fysieke wereld die we van oudsher (en nog steeds) kennen. Ook in de fysieke wereld is de overheid een participant die haar eigen rollen vervult (dienstverlener en handhaver om twee voorbeelden te noemen), haar eigen doelen nastreeft, maar ook kaders en voorzieningen biedt die nodig zijn om het maatschappelijk verkeer te laten functioneren. Daarbij kun je denken aan algemene juridische kaders als het Burgerlijk Wetboek en de Algemene wet bestuursrecht, maar ook aan identiteit: wie ben je en hoe kun je dat aantonen? De identiteitsketen van de overheid legt het fundament.

Dat begint heel fundamenteel bij de burgerlijke stand. Bij een geboorte erkent de overheid het bestaan van een mens en legt ook enkele identificerende gegevens vast. In Nederland worden die voor praktisch gebruik door de publieke en private sector opgeslagen in de basisregistratie personen (BRP). De overheid zet de BRP gegevens op documenten (paspoorten, identiteitskaarten) waarmee burgers in het maatschappelijk verkeer kunnen aantonen wie ze zijn. Ten behoeve van het economisch verkeer stelt de overheid ook vast dat bedrijven bestaan en legt identificerende gegevens vast in het Handelsregister. Opnieuw ten behoeve van publiek en privaat gebruik. Burgerlijke stand, BRP, identiteitsdocumenten en het Handelsregister zijn te beschouwen als bouwstenen waarmee de overheid burgers en bedrijven in staat stelt om met vertrouwen contacten te hebben en zaken te doen in de fysieke wereld.

In de fysieke wereld zijn dit soort basale voorzieningen en randvoorwaarden zo vanzelfsprekend dat we ons niet of nauwelijks bewust zijn van hun bestaan. Jammer genoeg zijn ze in de digitale wereld niet vanzelfsprekend aanwezig. Transacties verlopen anders in de digitale wereld. Daarom ziet het proces van digitaal inloggen er heel anders uit dan je bekend maken aan een fysieke balie en heeft authenticatie in de digitale wereld zich ontwikkeld tot een apart specialisme met eigen methoden en technieken. Op tal van punten moet opnieuw worden uitgevonden wat de rol van de overheid hierbij kan en moet zijn.

“De informatiesamenleving is een zeer complex geheel waarin burgers, bedrijven en overheid veel rollen vervullen, zeer verschillende doelen nastreven en met gebruikmaking van een grote diversiteit aan technische middelen met elkaar interacteren.”

Een inlogstelsel met drie verklaringen

Het bovenstaande levert twee redenen om de koers van het eID programma te verleggen: er ontstaan bijzonder hinderlijke gebruiksproblemen en de informatie-samenleving heeft meer nodig dan een overheid die middelen regelt voor het inloggen in het eigen domein.

Om daaraan tegemoet te komen stellen we voor weer terug te grijpen naar het ontwerp dat in 2014 voor het eID stelsel is gemaakt. Daarin wordt een inlogstelsel beschreven dat drie verklaringen kan leveren:

1. wie wil er inloggen (de dentiteitsverklaring),
2. wat mag deze persoon (de bevoegheids-verklaring),
3. welke gegevens betreft het (de attribuut-verklaring).

“Het inlogstelsel met de juiste functionaliteiten kan naar onze mening ook zo´n ´game changer´ zijn.”

Achter iedere verklaring zit een dienst die de betreffende verklaring moet opleveren. Het betreft diensten van heel verschillende aard die ieder hun eigen proces en vakmanschap vergen. Het is heel wat anders om een degelijk authenticatieproces dat voldoet aan de eisen van de eIDAS verordening voor betrouwbaarheidsniveau substantieel in te richten dan om een basisregistratie te voeren die betrouwbare geboortedatums kan leveren. Bevoegdheden definiëren en registreren is weer een ander vak. De drie verklaringen kun je zien als drie bouwstenen die in combinatie de informatie opleveren waar dienstaanbieders behoefte aan hebben wanneer iemand bij hen wil inloggen.

Waarom nu aandacht nodig?

Het lijkt misschien wat overtrokken om, op het moment dat het eID programma stevig onder druk staat om zo snel mogelijk identificatiemiddelen op te leveren, toch aandacht te vragen voor dit soort ontwerpvragen. Het zijn ons inziens echter heel cruciale, basale keuzes die nu gemaakt worden. Vergelijk het met de transportsector waar op zeker moment standaardmaten voor een container werden geïntroduceerd. De wereld van transport en logistiek is, net als de informatiesamenleving, heel complex met goederen van allerlei soort (duur of goedkoop, omvangrijk of klein, bederfelijk of niet), veel partijen met verschillende rollen en allerlei soorten transportmiddelen (schip, auto, trein, vliegtuig). Daar was de introductie van de standaard container een ´game changer´ die veel nieuwe ontwikkelingen mogelijk maakt. Het inlogstelsel met de juiste functionaliteiten kan naar onze mening ook zo´n ´game changer´ zijn.

De gebruiksproblemen oplossen door drie verklaringen te onderscheiden

We lichten de functionaliteit van de drie verklaringen toe die er ons inziens toe leidt dat de gebruiksproblemen zich niet meer voor hoeven te doen.

De identiteitsverklaring

De kern van elektronische identificatie, die uitgevoerd kan worden met verschillende middelen (pasje, een app, et cetera) is: welke persoon betreft het. Achter een identiteitsverklaring zit een register met geïdentificeerde personen en een stelsel met middelen waarmee personen kunnen aantonen wie ze zijn. De identiteitsverklaring vertelt een dienstverlener waar iemand wil inloggen welke persoon hoort bij het authenticatiemiddel dat is uitgereikt en welk betrouwbaarheidsniveau dat middel heeft. De attributen die aan de dienstverlener verstrekt worden kunnen variëren.
Dat kunnen unieke nummers zijn (het BSN binnen de overheid en een ander betekenisloosnummer zonder BSN buiten de overheid) maar ook andere identificerende gegevens. Er is geen enkele noodzaak om bepaalde identificerende attributen hard te koppelen aan een bepaald middel.

Dit betekent dat er geen onderscheid meer gemaakt hoeft te worden tussen middelen voor het publieke en het private domein. Afhankelijk van de dienstverlener waar wordt ingelogd, kunnen met een attribuutverklaring de correcte identificerende gegevens worden verstrekt. Eén middel is in principe bruikbaar voor alle transacties die in de informatiesamenleving voorkomen. Verplicht meerdere middelen gebruiken of opnieuw inloggen voor transacties in een ander domein kan vermeden worden.

De bevoegdheidsverklaring

Zodra duidelijk is wie wil inloggen moet gecheckt worden wat de betreffende persoon mag. Vooralsnog zijn daarbij vooral machtigingen in beeld geweest:

1. logt de persoon in namens zichzelf of voor een andere persoon en is hij daarvoor gemachtigd?

2. logt de persoon in als zichzelf (burger), namens een bedrijf (ondernemer) of bijvoorbeeld als erkend beroepsbeoefenaar, zoals een arts of een advocaat?

Naast deze machtigingen kan ook de centrale vraag vanuit de bescherming van persoonsgegevens als een bevoegdheidsvraag geformuleerd worden: welke gegevens mag deze persoon in welke gevallen aan welke dienstverlener ter beschikking stellen? Wanneer deze vraag beantwoord is, stelt de bouwsteen bevoegdheidsverklaring in het inlogstelsel ons in staat om de uitkomsten bij het inloggen te betrekken.

Door met bevoegdheidsverklaringen te werken is het niet meer nodig om onderscheid te maken tussen burgermiddelen en bedrijfsmiddelen. Dat geldt ook voor machtigingsvoorzieningen of MijnOverheid apart voor burgers en bedrijven. Burgers zijn vrij in het aantal middelen die ze aanschaffen en de doelen waarvoor ze die gebruiken. Wanneer ze eraan hechten om voor hun rol als werknemer een apart middel te gebruiken staat niets daaraan in de weg. Wanneer ze in de loop van de tijd van mening veranderen, staat niets nieuwe keuzes in de weg. Door ook de eisen die vanuit de bescherming van persoonsgegevens gesteld worden te vertalen naar een bevoegdheidsvraagstuk kan het inlogstelsel ook daarvoor faciliteiten bieden.

Attribuutverklaring

Met attributen bedoelen we de gegevens die bij het inloggen verstrekt worden. Een aparte verklaring brengt flexibiliteit in het inlogstelsel die het mogelijk maakt om op maat attributen te verstrekken. Het kunnen gevalideerde gegevens uit een welomschreven bron zijn (denk aan gegevens zoals: de geboortedatum uit de BRP), maar ook uit persoonskenmerken en afgeleide antwoorden op concrete informatiebehoeften van de dienstverlener (deze persoon is ouder dan 18 jaar) en wensen van de burger (het bezorgadres waar een nieuw paspoort kan worden uitgereikt). En identificerende gegevens (namen, nummers) zijn gewoon attributen waar per geval een optimale keuze uit gemaakt kan worden.

De conclusie van deze paragraaf is, dat het eID stelsel door de combinatie van attribuutverklaringen, identiteitsverklaringen en bevoegdheidsverklaringen het maatwerk leveren dat nodig is bij het inloggen in de vele verschillende situaties die in de informatiesamenleving voorkomen. Gebruikersproblemen die nu ontstaan worden vermeden.

“Door met bevoegdheidsverklaringen te werken is het niet meer nodig om onderscheid te maken tussen burgermiddelen en bedrijfsmiddelen.”

Een concreet voorbeeld: regie op gegevens

Het programma Regie op Gegevens (RoG) hanteert als vertrekpunt dat mensen inzage moeten hebben in hun persoonlijke gegevens en het gebruik daarvan door derden, dat zij de mogelijkheid moeten hebben om gegevens te corrigeren of te verwijderen en -niet in de laatste plaats- dat zij gegevens moeten kunnen (her)gebruiken, zowel binnen de overheid als daarbuiten. Zo wordt de positie van burgers versterkt.
Door hergebruik van gegevens te faciliteren worden burgers in staat gesteld als actor in de informatiesamenleving op te treden en zelf hun zaken te regelen. Sara is daar zeer mee geholpen.

Identiteitsverklaring

Wanneer Sara haar zaken in de informatiesamenleving wil regelen moet ze zich op het juiste betrouwbaarheidsniveau bekend maken. Dat er een identiteitsverklaring nodig is beschouwen we als een gegeven.

Attributen

Verder moet ze attributen kunnen verstrekken. Daar zijn centrale en decentrale modellen bij mogelijk die we in het buitenland ook allebei zien voorkomen. Centraal wil zeggen dat Sara voor hergebruik van overheidsgegevens aan de overheid vraagt om de gegevens namens haar te verstrekken. In Finland wordt met MyData voor zo´n centrale oplossing gekozen. Onze oosterburen kiezen voor een decentraal model, daar staan de belangrijkste attributen op de ‘Neue Personalsausweis’.

In Nederland wordt over beide modellen nagedacht. Het idee van een centrale attributendienst voor leeftijdsverificatie is wel eens uitgewerkt. Als Sara wil inloggen om drank te kopen of te gokken krijgt de dienstaanbieder niet alleen een identiteitsverklaring, maar ook een bevoegdheidsverklaring met een groen vinkje: Sara is ouder dan 18 en voldoet aan de gestelde leeftijdsgrens. Een decentrale variant is evenzeer denkbaar. Aan de Universiteit Nijmegen zijn de IRMA-kaart en -app ontwikkeld waarmee Sara zelf de identiteitsverklaring en ook de attribuutverklaring kan genereren. Daarvoor moet ze wel in haar persoonlijke data omgeving haar BRP geboortedatum beschikbaar hebben.

“Wanneer de bevoegdheidsverklaring nu op de juiste manier wordt gedefinieerd kan het inlogstelsel een middel zijn om daadwerkelijke verstrekkingen volgens de gestelde regels te laten verlopen.”

Het inlogstelsel kan beide modellen, ook tegelijkertijd, ondersteunen. Sara kan ermee inloggen bij de overheid om haar geboortedatum in haar persoonlijke data omgeving te laden. Ze kan de overheid vragen om namens haar een bevoegdheids-verklaring te genereren of dat zelf doen.

Bevoegdheden

Het lastigste punt bij regie op gegevens is de bevoegdhedenkwestie. Zoals gezegd betekent het feit dat een burger zelf handelt niet dat de regels voor de bescherming van persoonsgegevens niet meer gelden. Dat is maar goed ook. Partijen als Facebook, Apple en Google, maar ook talloze anderen zijn erop gericht maximaal gegevens over ons te verzamelen, ook wanneer dat volgens de regels van de AVG niet kan. Een privacykader met regels over welke gegevens in welke situatie met welke dienstaanbieders (binnen maar met name buiten de overheid) gedeeld kunnen worden, beschermt Sara tegen onbehoorlijke vragen. Hoe zo´n privacykader eruit moet zien, wordt door het inlogstelsel niet ingevuld. Wanneer de bevoegdheidsverklaring nu op de juiste manier wordt gedefinieerd kan het inlogstelsel wel een middel zijn om daadwerkelijke verstrekkingen volgens de gestelde regels te laten verlopen.

Onze conclusie is, dat voor regie op gegevens door burgers alle drie de functies van het inlogstelsel nodig zijn. Daarbij is werkverdeling mogelijk: wanneer het programma eID het inlogstelsel realiseert, hoeft het programma Regie op Gegevens alleen op te letten dat de eID faciliteiten aan haar eisen voldoen. RoG kan zich dan richten op het beschikbaar stellen van gegevens aan burgers en het ontwikkelen van kaders die burgers tegen onbehoorlijke informatievragen beschermen.

Consequenties voor het eID programma

Op korte termijn is het eID programma erop gericht zo snel mogelijk middelen om in te loggen in het BSN domein beschikbaar te kunnen stellen op de betrouwbaarheids-niveaus substantieel en hoog.
Om dienstaanbieders te ontzorgen komt er een routeringsvoorziening, zodat dienst-verleners nog maar met één koppelvlak en één beherende partij te maken hebben. Omdat dienstverleners gehinderd worden in hun ambities om nieuwe processen te digitaliseren, krijgt het realiseren van inlogmiddelen en de routeringsvoorziening prioriteit.

We beschouwen deze korte termijn doelstel-lingen van het programma als een gegeven. Om voor de langere termijn de doorontwik-keling naar een inlogstelsel met meer functionaliteit als mogelijkheid open te houden is het wel nodig om nu te besluiten tot het verbreden van het doel en de scope van het programma voor de langere termijn. Het uitgangspunt moet zijn dat in de behoeften van burgers en bedrijven wordt voorzien. Dat heeft meteen effect op het ontwerp van de routeringsvoorziening dat nu wordt opgesteld, op de doorontwikkeling van de machtigingsvoorzieningen en op te maken keuzes rond eHerkenning. Voor de goede orde: er wordt niet voorgesteld om op korte termijn te stoppen met eHerkenning. Wel om een inlogstelsel te realiseren waarin middelen niet meer per definitie aan een bepaald domein gebonden zijn en dat het de functionaliteiten biedt die nodig zijn in de informatiesamenleving. Dat is noodzakelijk om inloggen vanuit de overheid adequaat te ondersteunen.

Bronnen en verwijzingen

1 Werking van het eID stelsel versie 1.0. Januari 2014. BZK, programma eID, januari 2014.

2 https://www.digitaleoverheid.nl/beleid/naar-een-gegevenslandschap

3 https://www.digitaleoverheid.nl/dossiers/regie-op-gegevens

4 Identificatie en authenticatie in zorg en ondersteuning. CIO office ministerie van VWS, september 2016.

5 Factsheet Identificatie, authenticatie en autorisatie. Programma MedMij, augustus 2017

6 Verkenning impact regie op gegevens. VNG Realisatie, december 2017.

Over PBLQ

PBLQ is een adviesbureau dat zich richt op verandervraagstukken in de informatiesamenleving. In rap tempo transformeert Nederland naar een digitale informatiesamenleving waarin de overheid een cruciale rol speelt. Wij zijn specialist in het oplossen van verandervraagstukken waarbij de focus ligt op informatiemanagement in het publieke domein. Wij helpen onze opdrachtgevers met advies, traineeships en opleidingen.

Vragen en contact?

Heeft u vragen over dit whitepaper?
Neem contact op met **Dirk Schravendeel**

06 22 19 65 39
d.schravendeel@pblq.nl

Bezoekadres
Muzenstraat 120
2511 WB Den Haag

Postadres
Postbus 18607
2502 EP Den Haag

070 376 36 36
info@pblq.nl
www.pblq.nl

2018