Position Paper

Digitale Identiteit

Samen Organiseren, werkgroep Digitale Identiteit

1 Inwoner en bedrijf centraal, behoefte aan Digitale Identiteit

De samenleving verandert. Ook de verhoudingen tussen overheid, bedrijfsleven en de inwoner veranderen. De inwoner wil zaken kunnen doen op het moment en op de manier die hem schikken. Met bedrijven, met andere inwoners en met de overheid. Het is de uitdaging aan de overheid om de voorwaarden te scheppen dat de inwoner dat ook kan, overigens in samenspraak met andere maatschappelijke actoren. Zoals het rapport *Maak Waar* ook duidelijk aangeeft gaat het daarbij om denken en doen in samenhang. De verandering houdt ook niet op, dus de ook de dienstverlening van de overheid zal constant in beweging moeten blijven. *Permanent beta* in dienstverlening en ook de bijbehorende (al dan niet digitale) voorzieningen!

Wil de overheid zich niet buitenspel zetten in de informatiesamenleving, dan zal zij haar dienstverlening verregaand moeten digitaliseren en de publieke taken zodanig moeten inrichten dat de behoeften, vragen en voorkeuren van de inwoners centraal komen te staan. En dus niet het systeem, de openingstijden of de voorkeurskanalen van de overheid of haar samenwerkingspartners.

Om haar eigen dienstverlening beter te ondersteunen en aan te sluiten bij de maatschappelijke behoefte, is de introductie van een van een veilige, betrouwbare digitale identiteit dringend geweest. DigiD volstaat niet langer. Het heeft niet de status en het vertrouwen van het paspoort. Je kunt er geen hypotheek mee afsluiten, niet het rijbewijs mee verlengen, geen toeslagen of uitkering mee aanvragen en geen bankzaken mee afhandelen. En aan de telefoon of aan de balie heb je er niets aan.

Iedere persoon, of het nu burgers of organisaties betreft, heeft daarvoor een digitaal identiteit nodig naast de analoge. In organisaties begint dat in ieder geval met de bestuurders van die organisaties. Een digitale identiteit die bruikbaar is via alle kanalen die voor de dienstverlening worden gebruikt. Alle kanalen betekent dan ook het fysieke kanaal en het telefonische kanaal, naast diverse andere digitale kanalen zoals mobiele apps en klantcontact via chatfaciliteiten. Waarom? Denk dan aan alle dienstverlening die momenteel *niet* geleverd wordt via de telefoon (en die andere kanalen). Overheidsdienstverleners kunnen veelal geen persoonlijke gegevens bespreken in telefoongesprekken en al helemaal geen zaken doen, eenvoudigweg omdat de identiteit van de beller niet betrouwbaar (genoeg) kan worden geverifieerd. Het alternatief dat veel uitvoeringsorganisaties nu maar gebruiken bij klantcontact, het opvragen van

wat identificerende gegevens zoals een BSN en geboortedatum, is verre van betrouwbaar en leidt dan ook wel degelijk tot problemen in een aantal gevallen. Het kunnen beschikken over de mogelijkheid voor geauthenticeerd telefonisch verkeer lost deze problemen voor een aanzienlijk deel op.

Een soortgelijke beleving en klantreis is ook gewenst in het private domein. Hoewel in het private domein de diensten 'tegen directe betaling' grote vlucht hebben genomen (e-commerce) is dat minder het geval voor diensten waar een grote zekerheid over de identiteit van de digitale klant vereist is, zoals levering op afbetaling of het aangaan van langlopende verplichtingen.

Willen we zaken doen optimaal ondersteunen, dan zal de Digitale Identiteit het ook mogelijk moeten maken om stukken en transacties te kunnen accorderen met een rechtsgeldige ondertekening. En dit alles op een manier, waarbij de burger centraal staat en zelf de regie heeft op de dienstverlening en de daarvoor benodigde gegevens. De burger bepaalt dus wie welke gegevens krijgt voor welke doel en voor hoelang en dat begint met de (gegevens van de) Digitale Identiteit. Deze 3 elementen van de Digitale Identiteit, te weten

- 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 en
- regie op gegevens (en de diensten die de burger afneemt)

worden verderop in dit position paper verder uitgewerkt.

Het bovenstaande sluit nauw aan bij de door leden van de Regieraad Dienstverlening in 2016 uitgebrachte Visie op de dienstverlening 2025. Daarin wordt gewezen op de veranderende rol van de overheid en de noodzaak voor overheden om steeds meer samen te werken met andere maatschappelijke instituties en bedrijven. Gegevensuitwisseling tussen organisaties is dan vaak nodig. Deze gegevensuitwisseling onder de regie brengen van de inwoner kan hiervoor een privacyvriendelijke oplossing zijn.

Deels wordt de behoefte aan een digitale identiteit gedekt door ontwikkelingen als DigiD, eHerkenning en iDIN. We zien echter nog steeds een aanzienlijke ongedekte behoefte omdat dit in de praktijk alleen authenticatie op websites betreft. Ook blijft de beschikbaarheid achter van authenticatiemiddelen met een hoger betrouwbaarheidsniveau, nodig voor die diensten waar een grote zekerheid is vereist.

Wij, de gemeenten, bepleiten een voortvarende aanpak van Digitale Identiteit als fundament voor de bovengenoemde ontwikkelingen. Een Digitale Identiteit die net zo betrouwbaar is als onze analoge identiteitsdocumenten. Een digitale identiteit ook die in alle omstandigheden en soorten maatschappelijke interactie bruikbaar is. Dat laatste impliceert een bredere benadering van de digitale identiteit dan momenteel gezien met DigiD en het eID stelsel.

Wij zijn daarbij van mening dat de overheid voor die Digitale Identiteit dient te zorgen, omdat dit een natuurlijke taak is van de overheid en inwoners en bedrijven dat uiteindelijk ook van de overheid verwachten. Dit sluit rollen voor zakelijke dienstverleners in het leveren van gerelateerde producten en diensten op dit gebied overigens in het geheel niet uit. De keuze om deze taak bij de overheid te beleggen ligt voor de hand. De overheid vervult ook met betrekking tot de gewone identiteit een centrale rol in identiteitsvaststelling en het bieden van documenten en faciliteiten voor identiteitsverificatie. Het ligt dus voor de hand om dit door te trekken naar het digitale domein, zeker als we bedenken dat die beide domeinen in hoog tempo convergeren. De overheid volgt haar burgers immers met Burgerlijke Stand en Basisregistratie Personen (BRP) en aansluiting hierop is noodzakelijk: de gewone identiteit en de digitale identiteit zijn immers nauw aan elkaar gerelateerd. Ten tweede gaat het hierbij om een uiterst gevoelig onderwerp, waarbij grote zorgvuldigheid is geboden met het oog op fraudepreventie en bescherming van de persoonlijke levenssfeer. Oneigenlijke afwegingen die iets zouden kunnen afdoen aan die zorgvuldigheid, zoals een streven naar winstmaximalisatie, zijn hierbij ongewenst. Een zorgvuldigheid waarop ook democratische controle gewenst is. Ten slotte wijzen we erop dat in de eIDAS verordening lidstaten ook dienen in te staan voor elektronische identiteiten die grensoverschrijdend gebruikt kunnen worden. Dit suggereert dat de overheid ten aanzien van deze elektronische identiteiten op enigerlei wijze de eindverantwoordelijkheid moet kunnen nemen.

In de navolgende paragrafen werken wij dit nader uit. Tot besluit veroorloven we ons een kijkje naar die ontwikkelingen die het mogelijk maken voor de inwoners en bedrijven om veel meer 'aan de knoppen te zitten' waar het gaat om diens gegeven en de diensten die hij van de (semi-) overheid afneemt (regie op gegevens en dienstverlening). Dit is in een separate paragraaf uitgewerkt.

2 Hoe zou dat er voor die inwoner uit kunnen zien?

We zien dat de digitale identiteit in heel veel contacten een wezenlijke rol speelt. We spreken over de volgende categorieën, in willekeurige volgorde:

1. Inwoners met bedrijfsleven (Consumer-to-Business)
2. Inwoners onderling. (Citizen-to-Citizen)
3. De inwoner met de overheid (Citizen-to-Government) en het bedrijf met de overheid (Business-to-Government).
4. Overheden onderling (Government-to-Government. We bedoelen hiermee dat de medewerker van overheidsorganisatie A namens die organisatie zakendoen met een andere overheidsorganisatie B.)
5. Bedrijven onderling. (Business-to-Business)

Categorie 3 en 4 zijn tot op heden het onderwerp van overheidsinitiatieven geweest. Maar een Digitale Identiteit moet in al deze domeinen bruikbaar zijn en dient ontworpen te zijn om ook langs de verschillende kanalen te werken. Enkele voorbeelden zijn hieronder benoemd.

Casus kopen op afbetaling (categorie 1)

Een inwoner wil een auto kopen op afbetaling
Hij maakt alle papieren in orde via het internet na inloggen met behulp van zijn digitale identiteit. Zijn naam en adresgegevens worden ter beschikking gesteld aan de verkoper.
De inwoner ondertekent daarbij zowel de koopovereenkomst als een akte van lening digitaal.
Als hij de auto komt afhalen is de identiteit van de koper snel geverifieerd aan de hand van zijn digitale identiteit app.

Casus identiteit bewijzen bij wettelijke verplichtingen (categorie 1)

Op een aantal plaatsen legt de wetgever een verplichting op om identiteiten, al dan niet met aanvullende gegevens, van burgers vast te leggen. Neem bijvoorbeeld de verplichting met betrekking tot werknemers of uitzendkrachten. De verificatie kan, na wetswijziging, plaatsvinden aan de hand van de Digitale Identiteitsapp op de mobiele telefoon. De digitale identiteitsapp levert tevens een bewijs op dat de werkgever of de uitzendorganisatie dient te bewaren, waarmee latere controles mogelijk zijn.

Casus grotere betrouwbaarheid bij online koop (categorie 2)

Een inwoner wil iets kopen op Marktplaats. Omdat het gaat om een verkoper die ver weg woont, wil hij extra zekerheid over de identiteit van de verkoper. Doordat de verkoper met zijn Digitale Identiteit inlogt bij Marktplaats, is dat eenvoudig geregeld. Gaat het alsnog fout, dan verstrekt Marktplaats de benodigde gegevens van de verkoper zodat de koper toch zijn recht kan halen.

Casus dienstverlening aan balie (categorie 3)

Een inwoner komt aan de balie van het gemeentehuis voor een sociaal probleem. Hij wordt gevraagd zich te identificeren. De inwoner heeft echter geen identiteitsbewijs bij zich, maar kan zich met zijn Digitale Identiteits app op zijn mobiele telefoon alsnog identificeren.

Casus WMO (categorie3, meervoudig)

De inwoner doet een melding bij de gemeente en gebruikt daarbij zijn DigiD.
De gemeente maakt een afspraak voor een huisbezoek door een WMO-consulent.
De gemeente geeft een beschikking af en de noodzakelijke woningaanpassingen worden besteld bij een bedrijf.
De inwoner geeft na inloggen bij deze gemeente aan welke delen van zijn dossier met het bedrijf mogen worden gedeeld zodat het bedrijf het benodigde maatwerk kan leveren. De inwoner vult dat aan met medische details die het bedrijf nodig heeft.

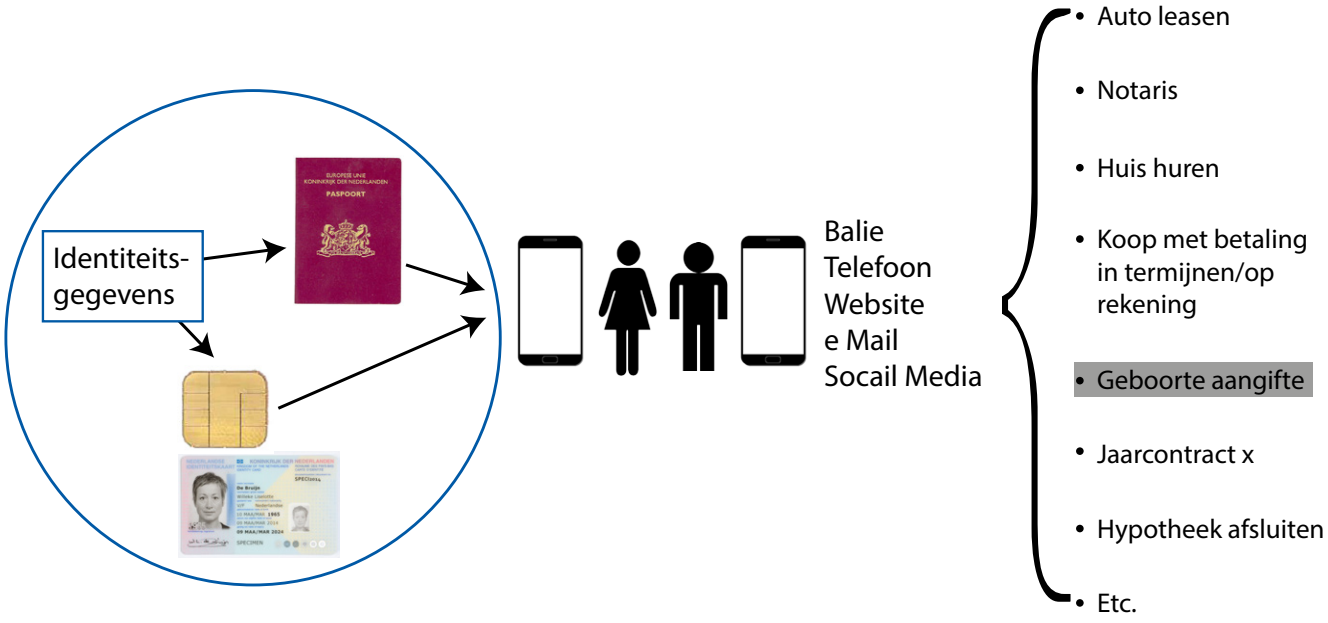
Casus telefonisch contact over rijbewijs (categorie 4)

Een medewerker van een gemeente constateert dat een rijbewijs niet zomaar kan worden aangevraagd en belt hierover naar het CBR. Omdat het om een persoonlijk geval gaat, mogen er alleen details gedeeld worden met bevoegde personen bij de gemeente. De medewerker gebruikt de digitale identiteit app op zijn mobiele telefoon om de gemeente en zijn rol in die gemeente te bewijzen aan de gesprekspartner bij het CBR.

Casus waterschap geeft vergunning af aan gemeente (categorie 4)

Een gemeente ontwikkelt een nieuwe wijk. Dit heeft ondermeer consequenties voor lozingen op het oppervlaktewater. De gemeente gebruikt haar digitale identiteit om een vergunning aan te vragen bij het waterschap hiervoor. Een bestuurder binnen de gemeente beschikt hiervoor over een authenticatiemiddel dit in de praktijk uit te voeren. De vergunning komt digitaal ondertekend door het waterschap retour.

Bovenstaande is weergegeven in de bijgaande figuur.



3 Wat hebben we daarvoor nodig?

Hierboven constateerden we al dat, om de inwoners en bedrijven werkelijk centraal te stellen en de toegankelijkheid goed te regelen, die inwoners en bedrijven de beschikking moet krijgen over:

1. Een middel om, langs in alle contexten en langs alle kanalen, te bewijzen dat hij is wie hij beweert te zijn (identificatie en authenticatie);
2. Een middel om, in ieder geval langs de verschillende schriftelijke kanalen, te ondertekenen en daarmee zijn wil te uiten (ondertekening).

De betrouwbaarheid van de Digitale Identiteit is hierbij van groot belang. Het voert te ver voor deze position paper om dat uit te werken. Maar wel kunnen we enkele uitgangspunten meegeven:

1. De betrouwbaarheid van de identificatie moet even goed zijn als die van een 'analoog' identiteitsdocument.
2. De beveiliging van de gegevens, zoals naam en pasfoto, moet op een hoog niveau liggen, dat is te vergelijken met de beveiliging van die gegevens op een identiteitsdocument.
3. De Digitale Identiteit kent een unieke koppeling met de identiteit van de houder, de natuurlijke persoon, en diens administratieve status in de officiële registers van de overheid (BRP, Burgerlijke Stand).
4. De verstrekking van gegevens uit de Digitale Identiteit staat onder de regie van de houder, vergelijkbaar met het fysiek aanbieden van een identiteitsdocument.
5. Verlies en diefstal van digitale identiteit worden onderkend en mogelijkheden worden geboden voor vlotte intrekking, alsmede nieuwe verstrekking.
6. De risico's die voortvloeien uit het misbruik van een digitale identiteit zijn voor de *relying party*, mits de houder zijn digitale identiteit zorgvuldig beheert.

Om te bepalen wat een vergelijkbaar risico precies inhoudt, is een ontwerp gevolgd door een nieuwe risicoanalyse nodig.

De betrouwbare identificatie en authenticatie (1) en een middel om digitaal te kunnen ondertekenen (2) zijn hieronder nader uitgewerkt. De daarbij gehanteerde definities zijn opgenomen in een bijlage op het eind van dit position paper.

1 Betrouwbare digitale identificatie en authenticatie

Betrouwbare digitale authenticatie is al heel lang een speerpunt van de Rijksoverheid. Al sinds 2004 hebben we DigiD en sinds 2010 hebben we ook eHerkenning. Dat dit niet alle behoeftes dekt is ook onderkend door het Ministerie van BZK, die met het Impuls eID-programma een wezenlijke stap voorwaarts op dit pad willen zetten.

Dit programma gaat uit van een **multimiddelenstrategie**, waarbij inwoners de beschikking krijgen over meerdere middelen waarmee zij zich kunnen authenticeren. Daarbij is een martkverdeling bedacht:

- Voor authenticatie bij publieke dienstverleners is een onderscheid te maken tussen burgers en medewerkers van organisaties. DigiD en een aantal toegelaten private authenticatiemiddelen zijn bruikbaar voor de burger. eHerkenning kan worden gebruikt door medewerkers van organisaties (privaat en publiek).
- Voor authenticatie bij private dienstaanbieders kan gebruik gemaakt worden van private authenticatiemiddelen. Desgewenst kan daar eHerkenning voor worden gebruikt.

De term multimiddelenstrategie duidt hierbij dus op het feit dat de burger alternatieven heeft naast DigiD. De oorspronkelijke gedachte hierbij was dat alle authenticatiemiddelen die aan een Uniforme Set van Eisen (USvE) voldoen, gebruikt kunnen worden door die burger om in te loggen bij publieke dienstverleners. Een vorm van 'open stelsel' dus.

Naast de behoefte voor alternatieven naast DigiD, bevat de strategie nog de realisatie van authenticatiemiddelen met een hoger betrouwbaarheidsniveau. Waar nu nog meer dan 80% van de dienstverlening van de overheid wordt ontsloten met het basisniveau van DigiD, een eenvoudige gebruikersnaam en wachtwoord, is het duidelijk dat dit betrouwbaarder moet. Dit wordt algemeen onderkend. Daarom wordt DigiD uitgebreid met de betrouwbaarheidsniveaus eIDAS Substantieel en Hoog. Het niveau eIDAS Hoog is vooral relevant voor toepassingen in de zorg, op de meeste andere plaatsen kan worden volstaan met eIDAS Substantieel of zelf Laag.

Naar aanleiding van diverse problemen met de oorspronkelijke multimiddelenstrategie heeft BZK de koers van het Impuls eID-programma bijgestuurd. De nadruk komt sterker dan voorheen te liggen op de doorontwikkeling van een publiek authenticatiemiddel. Geselecteerde marktmiddelen kunnen op basis van een aanbesteding wel worden toegelaten, zodat er wel een alternatief voor DigiD wordt geboden. Wij wijzen daarnaast nog op de volgende punten:

- Blijkens een onderzoek dat BZK heeft laten uitvoeren, *Communicatieonderzoek elektronische identificatie (eID),* van 23 mei 2017, begrijpen inwoners de multimiddelenstrategie niet. Bovendien kijken inwoners blijkens dit en andere onderzoeken voor hun digitale identiteit toch vooral naar de overheid. In ieder geval waar dat om authenticatie bij publieke dienstverleners gaat. Dat geldt ongetwijfeld ook voor een martkmiddel dat straks wordt aanbesteed.
- Inwoners zijn naar verwachting niet bereid om te gaan betalen voor een authenticatiemiddel of inlogacties, wat betekent dat de kosten voor het middel op een andere wijze gedekt moeten worden dan via een directe bijdrage door die inwoner.
- Er is voor zorgtoepassingen behoefte aan middelen op eIDAS Hoog. Het enige middel dat hiervoor op grote schaal beschikbaar komt, is DigiD Hoog. Het duurt echter circa 10 jaar voordat iedereen hierover kan beschikken.
- De scope van het Impuls eID-programma is simpel verwoord 'inloggen op een website'. Aan ondertekendiensten wordt ook nog wel gewerkt, maar van een brede ondersteuning voor identificatie en authenticatie via een veelheid aan kanalen (apps, chats, telefonisch, fysiek) is vooralsnog geen sprake.
- De behoefte aan vertegenwoordiging door een derde is aanzienlijk. Het gaat dan om vertegenwoordiging door professionals of door mensen in de directe persoonlijke kring om de betrokkene. In het programma Impuls eID is hiervoor zeker aandacht. De precieze voornemens op dit punt zijn echter een stuk minder helder.

Wij gemeenten worden in de praktijk geconfronteerd met deze behoeften en willen méér dan het huidige Impuls eID programma biedt:

1. Een identificatiemiddel, als onderdeel van de Digitale Identiteit, dat snel (wezenlijk sneller dan de te verwachten 10 jaar) hogere betrouwbaarheidsniveaus biedt, waarbij gedacht moet worden aan eIDAS Substantieel en eIDAS Hoog;
2. Een identificatiemiddel dat bruikbaar wordt voor toepassing in de private sector. We realiseren ons dat hiervoor bestaande afspraken opengebroken moeten worden, maar een brede gebruiksmogelijkheid is essentieel. Ongetwijfeld betekent dit ook dat DigiD aan private dienstaanbieders tegen marktconforme prijzen beschikbaar moet worden gesteld als inlogmethode.
   Een Digitale Identiteit die ook bruikbaar is op andere kanalen dan het inloggen op een website van de overheid.

Het laatste punt behoeft enige toelichting. We achten verbreding nodig van 'authenticatie op websites' naar 'betrouwbare digitale identificatie en authenticatie via alle kanalen'. Tot op heden werd de digitale dienstverlening veel via websites gedaan. Een moderne verschijningsvorm zou typisch een app op een mobiele telefoon kunnen zijn, waarmee een

inwoner zichzelf kan identificeren en authenticeren via het telefonische kanaal alsmede het fysieke kanaal. Immers, ook langs die kanalen vindt dienstverlening plaats en is een betrouwbare identiteit nodig. En in de toekomst verloopt het wellicht nog heel anders, waarbij wellicht de blockchain een centrale rol zal spelen. De basale behoefte aan identificatie authenticatie blijft, de vormgeving zal veranderen. Hetgeen het 'permanent beta' karakter eens te meer benadrukt.

Langs dezelfde gedachtlijn achten we het zinvol dat burgers kunnen beschikken over een alternatieve manier om zich in het fysieke domein te kunnen identificeren. Ook dit zou met een mobiele app kunnen plaatsvinden. Een mobiele telefoon heeft vrijwel iedereen altijd bij zich, een identiteitsdocument wordt nog weleens vergeten.

Onderdeel van dit concept, is dat de burger - door de overheid gevalideerde - identificerende gegevens kan leveren aan een dienstaanbieder. Ook het leveren van een foto kan dan zinvol zijn, bijvoorbeeld in het fysieke kanaal om *look-alike* fraude te vermijden.

2 Een digitale handtekening voor de inwoner en het bedrijf

In het verlengde van de identificatie en authenticatie langs *alle* kanalen achten we het ook nodig dat de inwoner wordt voorzien van middelen om langs de digitale weg ondubbelzinnig zijn wil te uiten en zich juridisch te binden. Voor het doen van serieuze zaken, zien we nu nog veel papier gebruikt worden. Denk aan contracten, polissen, koop op afbetaling. Of we zien een praktijk waarbij formulieren digitaal worden toegestuurd, worden geprint en ingevuld en ondertekend en dan weer gescand en per mail toegestuurd. Dit is een praktijk die noch gebruikersvriendelijk, noch betrouwbaar is.

De bestaande mogelijkheden voor ondertekening die de markt biedt, met name certificaten voor digitale handtekeningen, leveren nog een te grote drempel. Private ondertekendiensten, die op basis van authenticatiemiddelen werken, hebben een lagere drempel maar hebben nog te veel een niche-karakter.

Om een dergelijke digitale handtekening mogelijk te maken, stellen we op het standpunt dat het mogelijk moet worden om stukken te ondertekenen met de digitale identiteit en dat het ook mogelijk wordt om hiermee te ondertekenen in het private domein. Uiteraard tegen marktconforme voorwaarden om geen oneigenlijke concurrentie te introduceren (conform de Wet Markt en Overheid). Ook in het geval van een private dienstaanbieder wordt geen BSN geleverd, maar een pseudoniem en enkele identificerende attributen.

3 De rol van de overheid en de gemeente in het bijzonder

De gemeente speelt allereerst in het gebruik van de digitale identiteit (en personal data management) een belangrijke rol als dienstverlener. Immers, de gemeente moet haar diensten hierop inrichten. En omdat de gemeente zich steeds meer ontwikkelt als *het eerste loket van de overheid,* worden dat ook steeds meer diensten.

Naast 'gebruiker' van digitale identiteit is er een natuurlijke rol voor de gemeente in het leveren van de digitale identiteit. In de huidige praktijk heeft de gemeente een belangrijke taak in het leveren van de 'analoge' identiteit. De Burgerlijke Stand en het beheer van de BRP zijn bij de gemeente belegd. De aanvraag en uitgifte van reisdocumenten en rijbewijzen is bij gemeenten belegd.

Daarmee is de gemeente ook een gerede kandidaat om als aanvrager en uitgever van de digitale identiteit te gaan functioneren. Anders dan nu met DigiD het geval is, wordt met de komende generaties van DigiD (Substantieel en Hoog), gemikt op dienstverlening waar een hoge zekerheid is vereist in authenticatie. Dit vereist in het aanvraag- en uitgifteproces een identiteitsverificatie waarin er – tenminste voor DigiD Hoog en in een aantal gevallen ook voor DigiD Substantieel - direct contact is met de natuurlijke persoon in kwestie. En hiervoor is de gemeente als 'eerste loket van de overheid' wederom de aangewezen partij. Weliswaar wordt er geëxperimenteerd met andere processen voor de aanvraag en de uitgifte van reisdocumenten, waarbij andere overheidspartijen of private partijen de juiste procesgang en een betrouwbare identiteitsverificatie voorstaan. Waar inzet van andere partijen niet bij voorbaat is uit te sluiten, achter we het wel van belang dat dit gebeurt onder de verantwoordelijkheid van een overheidspartij en dat er toezicht is vanuit een overheidspartij. Gegeven de ervaring van gemeenten, achten we het logisch om de bovenstaande verantwoordelijkheid te beleggen bij gemeenten.

We achten het daarbij, om redenen van doelmatigheid en transparantie, gewenst om de uitvoering hiervan gezamenlijk op te pakken. We menen dat het eigenaarschap hiervan tenminste ten dele bij de gemeenten komt te liggen in samenwerking met de uitvoerders van de relevante GDI-componenten. Voor gemeenten liggen er concrete rollen in de

vraagarticulatie, aansturing en bewaking. We achten het uiterst gewenst om dit te gaan uitvoeren in het verband van Samen Organiseren. Voor de concrete ICT-ontwikkeling dient dan een gerede ontwikkelpartij te worden gezocht.

De digitale ontwikkelingen gaan dermate snel dat het zaak is snel te handelen. De urgentie is hoog en die wordt bij gemeenten en uitvoerder nadrukkelijke gevoelt. Verder uitstel zet ons op nog grotere afstand van landen als onder meer België en Estland die hier al jaren langer ervaring mee hebben. Het kan ook snel. Technisch zijn er mogelijkheden genoeg. Tegelijkertijd kan een begin worden gemaakt met het aanpassen van wet- en regelgeving die de e-samenleving in de weg staat, zoals de eis van een fysieke handtekening.

Is dat geregeld en beschikken burgers ook eindelijk over een veilige, unieke digitale identiteit dan kunnen er verdere stappen worden gezet naar een werkelijke e-samenleving. Maar, zoveel is zeker, zonder een digitale identiteit, geen e-samenleving.

4 Ontsloten perspectief: de burger 'aan de knoppen' van zijn gegevens en diensten

Eén van de belangrijkste zaken, waarvoor we de Digitale Identiteit willen toepassen, is het bieden van faciliteiten – een dashboard als het ware – aan inwoners en bedrijven om makkelijk(er) zaken te doen met de overheid. Onderstaande is hier uitsluitend opgenomen als een voorbeeld, omdat hiermee het belang van een Digitale Identiteit goed wordt geïllustreerd. Zonder een Digitale Identiteit is dit immers niet mogelijk. Het onderwerp zelf wordt met deze korte paragraaf echter geen recht gedaan. Op een geschikt later moment zal hiervoor een apart initiatief worden ondernomen.

'Burgers aan de knoppen' vraagt iets van een gereedschap bij de inwoners en bedrijven, waarmee die

1. het overzicht krijgen van de diensten waar hij voor in aanmerking komt,
2. het overzicht krijgen van lopende zaken. Ook van die zaken die over een keten van organisaties lopen zodat die burger de overdracht tussen organisaties kan bewaken. Denk bijvoorbeeld aan het aanvragen van een PGB, waarbij meerdere organisaties zijn betrokken en
3. het overzicht krijgen over gegevens die partijen voorhanden hebben en waarmee die – in toepasselijke gevallen - de gegevensuitwisseling tussen partijen kunnen besturen.

Dat ontslaat de dienstaanbieders nog niet van de verplichting om hun diensten, waar die voor de burger sterk aan elkaar zijn gerelateerd, beter op elkaar te laten aansluiten in een enkel dienstverleningsproces. Zo ontstaan op termijn wellicht ook 'organisatieoverschrijdende zaken'. Samenwerkingsverbanden dienen zich hierop te organiseren, zodat de dienstverlening die voor de inwoner of het bedrijf één geheel vormt, ook als één geheel wordt aangeboden en ervaren, ook al wordt de dienst in werkelijkheid door meerdere samenwerkende organisaties geleverd. Overbodige stappen vanuit het perspectief van burger of bedrijf dienen daarbij zo veel mogelijk worden geëlimineerd. Uiteraard vraagt dit ketenregie, waar wij als gemeenten graag aan bijdragen. De primaire verantwoordelijkheid voor deze ketenregie zal echter meestal elders liggen.

Bovenstaande sluit goed aan op de trend in Samen Organiseren, om de samenwerking van gemeenten met uitvoeringsorganisaties in de diverse ketens te bevorderen, bijvoorbeeld op het gebied van het Persoonsgebonden Budget (PGB). Bovenstaande sluit daarnaast ook goed aan bij de visie die in het kader van het BZK Project Regie op Gegevens wordt ontwikkeld, alsmede met de eerste beelden over de toekomstvisie voor MijnOverheid. Het gaat echter een stap verder, omdat het ook het concept van 'organisatieoverschrijdende zaken' introduceert. Wij achten dit essentieel in de – naar verwachting steeds vaker voorkomende - situatie dat de door de inwoner gewenste dienst door een keten of netwerk van partijen wordt geleverd. Wij bepleiten dan ook dat er in de governance op de eOverheid hier meer nadruk op komt te liggen.

De rol van gemeenten in het bovenstaande is zeer groot, niet zozeer vanuit het voeren van de ketenregie in de diverse ketens, maar wel om vanuit haar klantcontact de gevoelde knelpunten te signaleren. Overigens zullen we in de praktijk zien het bovenstaande een aanzienlijke transitie inhoudt. Niet elke inwoner beschikt immers meteen over dat 'dashboard', zodat er meerdere varianten van de dienstverlening enige tijd naast elkaar moeten blijven bestaan. Inwoners en bedrijven zullen dat individueel doen, op een voor hun passend moment.

5 Definities

Digitale Identiteit	De identificerende gegevens en de authenticatiemiddelen in een digitale vorm, waarmee een natuurlijke persoon of een rechtspersoon diens identiteit kan aanduiden en aantonen in verschillende contexten en langs verschillende kanalen. De contexten kunnen daarbij zowel publiek als privaat zijn. Kanalen kunnen daarbij verschillende onlinediensten zijn, maar ook het telefonische en het fysieke kanaal.
Dienstverlening	Het proces van het verlenen van een dienst door een dienstaanbieder, alsmede de geleverde dienst of het geleverde product zelf. Een dienstaanbieder kan een publieke organisatie zijn zoals een gemeente maar ook een private organisatie.
Authenticatie	Een elektronisch proces dat de bevestiging verzorgt van de elektronische identificatie van een natuurlijke persoon of rechtspersoon.
Authenticatiemiddel	Een aan een natuurlijke persoon of rechtspersoon gekoppeld middel, waarmee de authenticatie van die persoon mogelijk wordt gemaakt. Het middel is een materiële en/of immateriële eenheid die persoonsidentificatiegegevens bevat of ondubbelzinnig aanduidt.
Digitale handtekening	De implementatievorm van de elektronische handtekening, gebaseerd op public key technologie. In dit stuk wordt verondersteld dat dit een geavanceerde of een gekwalificeerde elektronische handtekening (conform de eIDAS verordening) betreft.
Elektronische handtekening	Gegevens in elektronische vorm die gehecht zijn aan of logisch verbonden zijn met andere gegevens in elektronische vorm en die door de ondertekenaar worden gebruikt om te ondertekenen.
Personal Data Management	Het beheren van persoonlijke gegevens, hun verwerking en terbeschikkingstelling aan dienstverleners door de betrokken persoon. Het is de technische term voor 'regie op gegevens'.
Personal Data Service	Een dienst die personal data management mogelijk maakt.

oktober 2017