Initiatieven en Stelsels
Personal Data Management

Overzicht en inzicht

AUTEURS Laura Claas
Marlies Rikken
Wil Janssen
PROJECT REFERENTIE Programma Regie op Gegevens
STATUS Definitief – versie 1.4 – 10/11/17

Inhoud

Managementsamenvatting

Persoonlijk datamanagement heeft al een lange historie in Nederland en daarbuiten. De basis voor MijnOverheid werd meer dan 12 jaar geleden gelegd, Qiy is gestart in 2007, hetzelfde jaar dat Mydex in het Verenigd Koninkrijk werd opgericht. Sinds die tijd is er veel gebeurd, maar een echte doorbraak is uitgebleven. MijnOverheid is ver weg gebleven van de oorspronkelijke ambities, met Qiy hebben enkele pilots gelopen, maar opschaling ontbreekt nog. Wat wel werkt tot nu toe zijn smalle toepassingen als het pensioenoverzicht. Maar PDM-diensten in de breedte missen nog. Tegelijk zien we de laatste paar jaar een explosie aan initiatieven, met name vanuit verschillende toepassingen. Ontwikkeling in de raamwerken zit met name ook in de specifiekere raamwerken, zoals Idensys voor identificatie en MedMij in de zorg.

Toepassingen zitten een veelheid aan domeinen. Verzekeraars hebben samen de Poliskluis ontwikkeld die dit jaar wordt uitgerold, The Moneyer aggregeert bankgegevens, Tippiq stelt je huis centraal, CV monitor valideert je CV. En zo hebben we tientallen voorbeelden gevonden, zonder dat we compleet zijn. Ook de hausse aan fintech innovaties, onder andere aangejaagd door PSD2 wetgeving, leidt tot initiatieven op financieel vlak, zoals Leaflad, Dime en Schluss.

De aard van de toepassingen varieert sterk, net als de volwassenheid: sommigen hebben een maatschappelijk doel, anderen zijn volledig commercieel. Sommigen streven naar open source en open kennis, anderen zijn zakelijke diensten. Dat maakt vergelijken moeilijk. Om een indicatie te geven noemen we een aantal initiatieven en hun positionering in onderstaande tabel.

Tabel 1: Overzicht van een aantal initiatieven

Initiatief	*Horizontaal*	*Verticaal*	*Concept*	*Pilot*	*Operationeel*
Dappre	x				x
IRMA	x			x	
Leaflad	x			x	
Only Once	x			x	
Schluss	x			x	
Cleverbase	x			x	
Ydenti	x				x

AFAS Personal		Financiën			xx
Poliskluis		Verzekeringen			x[1]
CV Monitor		Werving			xx
LSP		Zorg			xxx
Mijn Pensioenoverzicht		Pensioen			xxx
MijnOverheid		Overheid			xxx
The Moneyer		Financiën			xx
Tippiq		Wonen			x
DataPlaza		Wonen		x	
HealthSuite (Philips)		Zorg		x	
Ockto		Financiën		x	
Social JO!N		Sociaal domein		x	
Dime		Advertenties	x		
Financieel paspoort		Financiën	x		

Met andere woorden een grote diversiteit aan domeinspecifieke initiatieven, in een sterke variatie aan volwassenheid. Daarmee groeit de noodzaak voor een verantwoord raamwerk voor persoonlijk datamanagement. Zonder dat kader kunnen initiatieven leiden tot situaties die voor burgers/consumenten, dataleveranciers en dienstverleners tot zorgelijke situaties leiden, waarbij misbruik en datalekken op de loer liggen.

De ontwikkeling van afsprakenstelsels gaat in het algemeen langzamer en het aanbod is beperkter. Het Qiy afsprakenstelsel is in ontwikkeling sinds 2006 en de ontwikkeling loopt nog door. Specifiekere afsprakenstelsels gaan wat sneller, zo lijkt het. Idensys (eerder eID) is vrij snel tot stand gekomen en ook MedMij in de zorg pakt snel momentum. Beide stelsel lijken de vruchten te plukken van de ervaringen van de afgelopen tien jaar om tot goede keuzes te komen. Rond Idensys en iDIN heeft de overheid ook duidelijke kaders gegeven voor toelatingseisen, al zijn beide natuurlijk wel beperkt in hun functionaliteit.

Tabel 2: Overzicht belangrijkste PDM raamwerken

Afsprakenstelsel	*Horizontaal*	*Vertikaal*	*Concept*	*Toegepast*	*Brede adoptie*
Qiy Foundation	x			x	
TrustTester	x		x		
Idensys		Identiteit			x
iDIN		Banken			x
MedMij		Zorg		x	
UETP		Transacties	x		

Internationaal spelen er ook een aantal belangrijke ontwikkelingen: Estland staat inmiddels bekend als een gidsland op e-overheid gebied. Finland trekt hard aan Mydata als concept en in de slipstream daarvan groeien de initiatieven snel. Beide worden sterk gedreven door een noodzaak en visie vanuit de overheid. In het Verenigd Koninkrijk timmert Mydex al lange tijd aan de weg rond Personal Data Management. Ze hebben, als not-for-profit bedrijf (CIC) een volwassen trust framework sinds een aantal jaren en een aantal toepassingen

[1] Verzekeraars worden nu aangesloten. Eind 2017 beschikbaar voor consumenten

live, inclusief een berichtenbox en personal data service. Ook zij worstelen echter met de opschaling en brede adoptie.

De vraag is nu welke lessen we kunnen trekken uit de verschillende initiatieven. Is er een relatie te leggen tussen de aard van het initiatief en het succes of het tempo van uitrol?

In elk geval kun je stellen dat de eerste initiatieven last hebben (gehad) van het moment van introductie. MijnOverheid en Qiy waren vroeg. Hyves is in 2004 opgericht en stond nog in de kinderschoenen. Facebook en Linkedin bestonden al maar waren in Nederland nog onbekend. Data delen was een nieuw fenomeen. Smartphones bestonden nog niet. In dat tijdgewricht liepen ze ver voor de troepen uit. Nieuwere partijen kunnen dan profiteren van de eerdere ervaringen. Je heb geen “first mover advantage”, maar juist een “second mover advantage”.

Een tweede aandachtspunt is een sluitend bedrijfsmodel. Hoe financier je een ontwikkeling? Veel van de goedlopende initiatieven hebben een eenvoudig model, bijvoorbeeld gefinancierd door een collectief of de overheid (pensioenoverzicht, poliskluis) of vanuit een zakelijke dienst (CV Monitor, The Moneyer). Zonder een duurzaam bedrijfsmodel is het moeilijk om tot een doorbraak te komen. Daarbij kan het bedrijfsmodel in de ontwikkelfase anders zijn dan in de opschaling, maar het moet wel helder zijn, juist ook voor de gebruiker.

Daarnaast spelen transparantie en vertrouwen een grote rol. Gegeven dat het om persoonlijke data gaat is vertrouwen een belangrijk goed. Hoe generieker de oplossing, hoe meer vertrouwen nodig is. Een specifieke oplossing in een smal domein kan toe met een beperktere vertrouwensbasis. Transparantie geldt zowel voor de inhoud als voor het achterliggende governance- en bedrijfsmodel.

Vertrouwen wordt ook versterkt door wetgeving of een goed kader. Het pensioenregister heeft een wettelijke basis, Idensys heeft een helder kader, MijnOverheid krijgt dit met de GDI ook in sterkere mate. Soms lijkt wetgeving in eerste instantie een ontwikkeling te bevorderen, maar liggen risico’s in de implementatie. Daar waar de GDPR direct geldig is in alle lidstaten, zijn in de uitwerking van de PSD2 de nodige verzwakkingen opgetreden die de oorspronkelijke doelen in de weg staan. Een overheid moet daarin stevig in haar schoenen staan en weten welke visie op PDM of e-dienstverlening in het algemeen zij voor staan.

Een lichtere rol voor de overheid, of voor branche-organisaties, ligt in de standaardisatie van gegevens. De zorg is daarin ver (HL7 e.a.) en standaardisatie was essentieel in het uniform pensioenoverzicht. Zonder standaardisatie is uitwisseling van gegevens moeilijk: de betekenis ontbreekt. Dit is nadrukkelijk een probleem in de meer generieke stelsels. Met de genericiteit verdwijnt de betekenis.

Een andere factor die uitrol in de weg heeft gestaan is een goede identiteitsprovider. DigiD bestaat al lang, maar toepassingen beperken zich tot het BSN-domein. Dit leidde tot een wildgroei aan toegangscodes voor elke Mijn Omgeving waar je gebruik van wilde maken, van je pensioen tot je verzekeraar en je energieleverancier. Met social login (gebruik van Facebook, Linkedin e.a.) wordt dit hiaat ingevuld voor risico-arme toepassingen die beperkt persoonsgegevens gebruiken. Hiervoor is de standaard Oauth2.0 beschikbaar en breed geadopteerd. iDIN kan in private toepassingen een rol gaan spelen en Idensys middelen en hoger niveau DigiD zal toepassingen met gevoeligere persoonsgegevens gaan faciliteren. We groeien naar een situatie van “bring your own ID” – je kiest zelf met welk middel je in welke situatie je bekendmaakt.

Samenvattend zien we dat specifiekere oplossingen, gesteund door open standaarden of domein standaarden, met een transparant doel en bedrijfsmodel op dit moment de beste papieren in huis hebben. Start bij een (domeinspecifieke) vraag en voeg waarde toe. Maar baseer dat op een hoogwaardige infrastructuur die vertrouwen versterkt.

1 PDM in context

1.1 VRAAGSTELLING

Ongeremde uitwisseling van persoonsgegevens, het is een gegeven. Het blijft moeilijk om grip te krijgen op de hoeveelheid gegevens die organisaties over personen verzamelen. Het individu moet een keuze krijgen, en zelf kunnen bepalen wie zijn gegevens mag inzien. Regie op Gegevens wakkert de maatschappelijke dialoog over Persoonlijke Data Management (PDM) aan, door onderzoeken en discussies (Programma Regie op Gegevens (2016) *Persoonlijke Data Management*).

Inmiddels zijn er steeds meer initiatieven die een poging doen om de regie terug te leggen bij de bron: de persoon over wie de gegevens gaan. Beleidsvraagstukken rond privacy en beveiliging spelen hierin een grote rol. Afspraken stelsels als Qiy en Medmij proberen de spelregels rond uitwisseling van data vast te leggen.

Maar er zijn ook al services die met een directere aanpak het individu centraal te stellen. Bijvoorbeeld DataPlaza levert een platform waar personen via een beveiligd portaal dossiers kunnen uitwisselen met notarissen. Zo zijn er ook in andere sectoren initiatieven, zoals Tippiq in de huizenmarkt, de CV Monitor en The Moneyer voor financiële gegevens.

Dit rapport draagt bij aan deze discussie door het landschap van oplossingen en afsprakenstelsels rond PDM in kaart te brengen en inzicht te bieden in de betekenis van deze ontwikkelingen.

1.2 AFBAKENING

In dit rapport creëren we een overzicht van de ontwikkelingen in het veld. We kijken hierbij naar trust frameworks, initiatieven en behoeftestellers. Zowel publiek als privaat, met een focus op initiatieven binnen Nederland of met grote impact op Nederland. Op basis van het overzicht van ontwikkelingen worden inzicht vergaard. Zijn er patronen te ontdekken in de analyse van de initiatieven? Wat werkt er wel en wat werkt er niet? Wat kunnen we hieruit leren?

Om het overzicht behapbaar te maken, verdelen we PDM-ontwikkelingen in twee smaken: PDM afsprakenstelsels en PDM oplossingen.

Definitie afsprakenstelsels: Afsprakenstelsels bevatten de onderliggende standaarden om personal data services mogelijk te maken. Ze doen uitspraken over bijvoorbeeld data minimalisatie, validatie van bronnen, consent en overdraagbaarheid van data. PDM afsprakenstelsels zijn specifieke instanties van een trust framework.

Definitie oplossingen: Oplossingen zijn voornamelijk PDM-services, "diensten die een individu in staat stellen om zijn persoonlijke informatie duurzaam te beheren en te onderhouden " (Digital We (2015) *Eigen Data Delen).*

Een oplossing kan gebaseerd zijn op een specifiek afsprakenstelsel, maar dat hoeft niet. Vaak zijn de onderliggende afspraken grotendeels impliciet, of zijn te achterhalen via elementen in de gebruiksvoorwaarden. Bij een oplossing als Dappre wordt duidelijk aangeven dat het gebaseerd is op het Qiy afsprakenstelsel. Bij Mydex zijn de oplossing en het onderliggende stelsel transparant gescheiden.

Persoonlijk Data Management heeft betrekking op de manier waarop een persoon beschikking heeft over zijn/haar persoonlijke data. De persoon over wie de gegevens gaan staat hierin centraal. Via persoonlijke data services wordt het voor personen makkelijker om persoonlijke data, die bij verschillende data aanbieders staat, in te zien, te wijzigen en verwijderen. Dit wil niet per sé zeggen dat de PDS zelf data zal opslaan; dit is wel een mogelijkheid en afhankelijk van de PDS. Daarnaast maken PDS het mogelijk om voorkeuren voor toegang tot de data te bepalen. Service aanbieders kunnen toegang vragen tot de data om persoonlijke aanbiedingen te leveren. Door persoonlijk datamanagement toe te passen kan waarde worden gecreëerd, voor de persoon en voor de partijen in het PDM netwerk, met een manier waarop persoonlijke data beschermd blijft.

Om dit te realiseren is er een open infrastructuur nodig waarop de data beveiligd uitgewisseld kan worden. Daarnaast is de beveiliging van deze infrastructuur een eis; authenticatie en autorisatie zijn nodig voor organisaties en personen om data uit te kunnen wisselen. Er is een stuk governance nodig, onder andere in de vorm van afsprakenstelsels, om te bepalen welke rollen er zijn en door welke partijen die worden vervuld, hier zal de overheid ook een rol in spelen. Wie is op welk moment verantwoordelijk voor de data? Hoe verloopt de uitwisseling en welke authenticatiediensten en identificatiemiddelen mogen gebruikt worden? Rechten, plichten en mogelijke sancties horen hier ook bij.

Tabel 1. Begrippenlijst PDM.

Begrip	***Uitleg***	***Bron***
Anoniem (of: geanonimiseerd)	Niet traceerbaar naar de persoon	Qiy Foundation (2015) *Definitions of the Qiy Scheme v1.0*
Authenticatie	Het aantonen dat degene die zich identificeert ook daadwerkelijk degene is die zich als zodanig voorgeeft. Authenticatie noemt men ook wel verificatie van de identiteit.	Ministerie van BZK (2012) *NORA 3.0 Principes voor samenwerking en dienstverlening*
Authenticatiedienst	Verantwoordelijke service voor het authentiseren van personen.	
Autorisatie	Het proces van het toekennen van rechten voor de toegang tot geautomatiseerde functies en/of gegevens in ICT-voorzieningen	Ministerie van BZK (2012) *NORA 3.0 Principes voor samenwerking en dienstverlening*

Data aanbieder	Een organisatie die persoonlijke data opslaat en beheert en dit beschikbaar kan stellen aan service aanbieders.	Qiy Foundation (2015) *Definitions of the Qiy Scheme v1.0*
Open infrastructuur	Infrastructuur waarop service aanbieders, data aanbieders en PDM-services op een gestandaardiseerde manier kunnen aansluiten.	
Persoon	Natuurlijk persoon of ondernemer.	The Sovrin foundation (2016) *Sovrin: Glossary of terms*
Persoonlijke data	Data die is gerelateerd aan een natuurlijk persoon, zoals adres en telefoonnummer. Persoonlijke data gaat ofwel direct over een persoon, of is tot een persoon te herleiden. Persoonlijke data kan ook over een onderneming gaan.	Qiy Foundation (2015) *Definitions of the Qiy Scheme v1.0*
Persoonlijk Data Management (PDM)	Het concept rond het duurzaam beheren en onderhouden van persoonlijke data.	Digital We (2015) *Eigen Data Delen*
Persoonlijke data management afsprakenstelsel (PDM afsprakenstelsel)	Set van vastgelegde afspraken om samenwerking en zekerheid te garanderen op het gebied van technische functionaliteiten, beveiliging en privacy voor het uitwisselen van persoonlijke data.	
Persoonlijke data management service (PDM service)	Een dienst die een individu in staat stelt om zijn persoonlijke data duurzaam te beheren en te onderhouden om deze, wanneer de gebruiker dit in zijn belang acht, te kunnen delen met anderen.	Digital We (2015) *Eigen Data Delen*
Service aanbieder	Een organisatie die diensten aanbiedt, welke gebruik maakt van persoonlijke data.	Qiy Foundation (2015) *Definitions of the Qiy Scheme v1.0*
Trust framework	"A legally enforceable set of specifications, rules, and agreements that govern a multi-party system established for a common purpose, designed for conducting specific types of transactions among a community of participants, and bound by a common set of requirements. "	Makaay et al. (2017)

1.3 LEESWIJZER

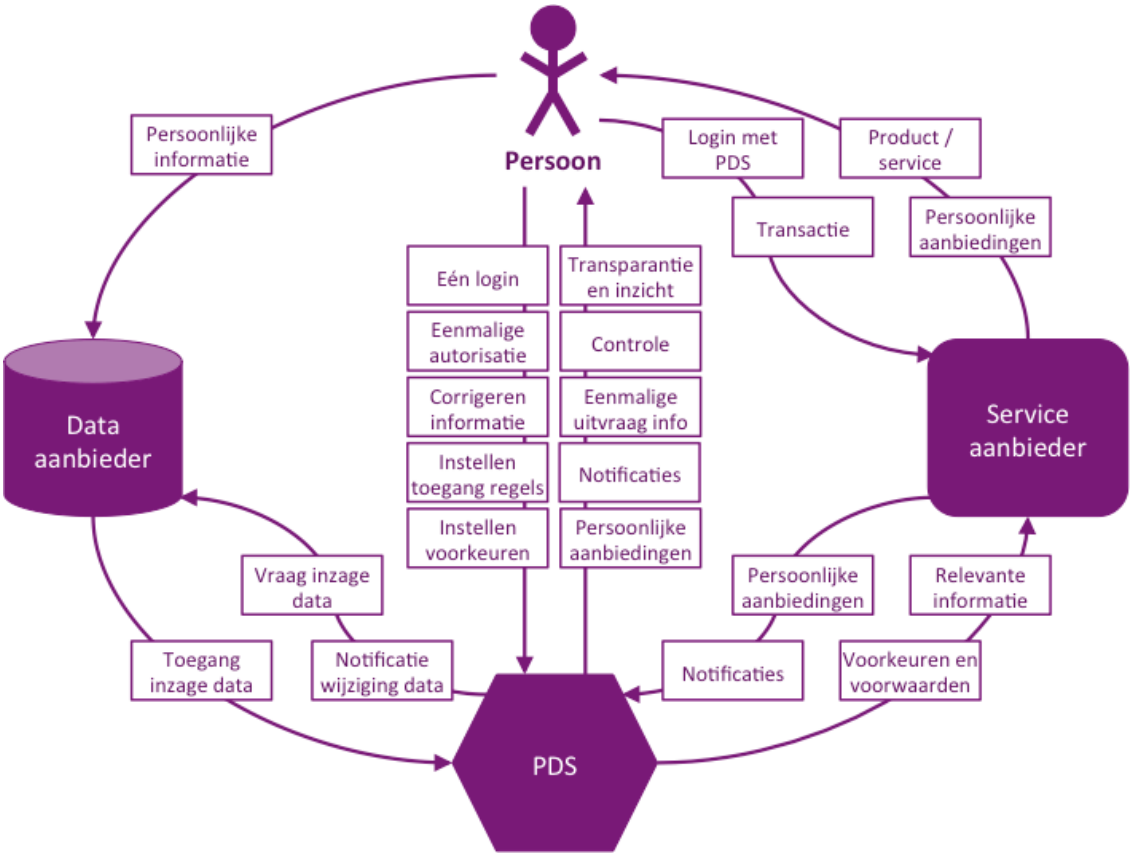
Het rapport geeft eerst een generiek beeld van PDM; wat personal dataservices zijn en welke componenten ze kunnen hebben. Dit is te vinden in hoofdstuk twee. Hoofdstuk drie bevat de longlist van op dit moment relevante initiatieven in Nederland. Deze is opgedeeld in drie categorieën: initiatieven, trust frameworks en internationale initiatieven. In hoofdstuk vier wordt deze longlist geanalyseerd en een aanzet gedaan tot implicaties. Hoofdstuk vijf gaat dieper in op de analyse, beschrijft welke patronen er te vinden zijn in de analyse en wat we hieruit kunnen leren. In hoofdstuk zes is te vinden wat de implicaties zijn van de analyse. Wat zijn de conclusies en wat betekenen de observaties voor de rol van de overheid?

2 Componenten van PDM

2.1 FUNCTIONALITEIT

Hoe zou het netwerk rond personal datamanagement eruit kunnen zien? Welke rollen zijn er, welke waarde wordt er uitgewisseld? Onderstaande afbeelding en uitleg geven een duiding hoe dit netwerk zich zou kunnen ontwikkelen. De persoon op wie de data in het netwerk betrekking heeft staat hierin altijd centraal. In het waarde netwerk rondom Personal Data Services zijn er vier rollen te vervullen:

- Personal Data Service
- Data aanbieders
- Service aanbieders
- De persoon aangesloten bij de PDS: de gebruiker



Afbeelding 1: Waardenetwerk PDM

Personen hebben persoonlijke data bij verschillende data aanbieders staan. Daarmee heeft de persoon meestal een bepaald contact, zoals banken die beschikken over rekeningnummers of de Belastingdienst die beschikt over inkomensgegevens. Hij heeft veel van deze data aanbieders en zijn persoonlijke data staat daarom erg verspreid in het netwerk van de gebruiker.

De personal dataservice zorgt ervoor dat er meer overzicht ontstaat in die verspreide persoonlijke data. Welke data bestaat, en bij welke aanbieder, wordt inzichtelijk gemaakt. De gebruiker heeft één inlog bij de PDS, waarmee hij van meerdere data aanbieders beschikbare informatie kan bekijken. Dit wil niet direct zeggen dat de PDS zelf data zal opslaan, dit is wel een mogelijkheid en afhankelijk van de PDS.

Tussen de PDS en de data aanbieder zal een autorisatie nodig zijn, zodat de PDS een verzoek voor inzage bij de data aanbieder kan doen. Afhankelijk van de PDS en de betreffende data is het mogelijk om de informatie te corrigeren, die vervolgens een notificatie stuurt aan de data aanbieder dat er een wijziging in de data is. Het is

aan de gebruiker om te in te stellen voor welke data aanbieders er connectie gemaakt wordt met de PDS, wie welke informatie ziet en waar de informatie gebruikt mag worden.

Een service aanbieder kan allerlei diensten verrichten op basis van de data van de gebruiker. Een mogelijkheid is het ontvangen van persoonlijke aanbiedingen. Op basis van de voorkeuren en instellingen van de gebruiker kan de service aanbieder informatie krijgen, waardoor de gebruiker persoonlijke diensten krijgt. Via de PDS kan er, als de gebruiker op de aanbieding ingaat, een transactie verlopen.

Een andere mogelijkheid is inloggen in de omgeving van de service-aanbieder. Afhankelijk van de voorkeuren van de gebruiker kan de service-aanbieder gebruik maken van data via de PDS. Wanneer de gebruiker hiermee akkoord gaat kan de service aanbieder op zijn eigen omgeving persoonlijke aanbiedingen creëren. Ook in deze situatie zal er direct met de service aanbieder een transactie plaatsvinden.

2.2 FICTIEVE USE CASE

Laten we een voorbeeld geven van het gebruik van een “ultieme PDS”, een fictief voorbeeld, waarin publiek en privaat gebruik worden gecombineerd. Een animatie van deze use case is ook beschikbaar.[2]

> *Eva Jansen en Guus Cornelis staan op het punt om een huis te kopen. Jarenlang hebben ze gehuurd. Guus heeft een VOF samen met een vriend en Eva is zelfstandig adviseur, waardoor het een risico was om te investeren in een huis. Maar nu is hun droomhuis beschikbaar en willen ze het graag kopen. De jaarrekeningen van Eva en Guus staan bij elkaar in hun digitale dossier, PDS-Pro. In PDS-Pro beheren ze hun financiële zaken, samen met de accountant en de boekhouder. Sinds een paar jaar kunnen de gegevens van alle bankrekeningen hierin worden gecombineerd met de andere gegevens. PDS-Pro is door Eva en Guus geautoriseerd om alle overheidsinformatie rond de bedrijven en hen persoonlijk te ontsluiten. KvK gegevens, GBA en belastingaangiftes zijn dus bij elkaar beschikbaar.*
>
> *Na een kort gesprek met Eigen Huis besluiten ze om een viertal hypotheekverstrekkers een offerte te vragen. In PDS-Pro worden Interpolis, Florius, een Duitse en een Estse hypotheekverstrekker uitgenodigd te offreren. Daartoe mogen de hypotheekverstrekkers de relevante gegevens drie dagen inzien en moeten ze binnen vijf werkdagen offreren. Ze betalen een commissie aan PDS-Pro voor de mogelijkheid om een persoonlijke offerte te sturen naar potentiële klanten. ’s Avonds bekijken Eva en Guus de voortgang. Drie van de vijf hebben gegevens al bekeken; de Estse hypotheekverstrekker vraagt of ze een combinatie mogen aanbieden met een woonzekerpakket. Dat mag. De anderen worden geïnformeerd dat die optie er is. Uiteindelijk is het Duitse aanbod het meest aantrekkelijk. Op de woonverzekering gaan Eva en Guus apart laten bieden, los van de hypotheek. Op 12 juli krijgen ze de sleutel van het huis en beginnen ze met een kleine verbouwing en veel schilderwerk. Gelukkig zijn er veel vrienden die de helpende hand reiken.*
>
> *Op 17 juli krijgen ze bericht in PDS-Pro van de Belastingdienst die aangeeft dat ze de aankoop hebben gezien en de hypotheekgegevens hebben bekeken. Voorstel is om de hypotheekrenteaftrek maandelijks te verrekenen. Als het akkoord is wordt de eerste termijn 23 juli bijgeschreven. Meteen plannen Eva en Guus de housewarming party op 1 augustus.*

In deze situatie is de burger of het bedrijf zelf regisseur van de informatie, publiek en privaat. Regie betekent sturing op wie welke informatie ziet, voor welk doel en met welke prijs. Informatie die publieke organisaties hebben kan door de burger of het bedrijf gedeeld worden met private partijen onder voorwaarden, zoals een beperkte tijd, specifieke doelen of specifieke combinaties. De consument/burger kan dus informatie uit het publieke domein ontsluiten voor private doeleinden. Immers, het is zijn of haar informatie. Omgekeerd kan, als dat gewenst is, ook privéinformatie gedeeld worden met de overheid. Denk aan situaties als werkloosheid of schuldsanering, waarin privébezit en overheidsdiensten gecombineerd worden.

[2] Zie https://youtu.be/OjQSBm3Nkf0

3 Afsprakenstelsels en oplossingen

Wat speelt er allemaal rond PDM? Wat is de status van PDM-oplossingen? Wat kunnen we de komende tijd verwachten van afsprakenstelsels in PDM? In dit hoofdstuk geven we een overzicht van de ontwikkelingen in het veld. Zowel publieke als private initiatieven worden in dit overzicht meegenomen. De focus ligt op oplossingen binnen Nederland of met (mogelijk) grote impact op PDM-ontwikkelingen. Het is bijna onmogelijk om volledig te zijn in dit overzicht. De auteurs houden zich dan ook aanbevolen voor missende oplossingen en ontwikkelingen. In paragraaf 3.3 bespreken we ook een beperkt aantal buitenlandse ontwikkelingen.

In de appendix (Alexandre de Montjoye et al. (2014) openPDS: Protecting the Privacy of Metadata through SafeAnswers. PLOS One, Beschikbaar via: https://doi.org/10.1371/journal.pone.0098790.

Analyse van afsprakenstelsel Qiy (2016) *Rapport van bevindingen*

Clippinger, J.H, & D. Bollier (red.). (2014) From bitcoin to burning man and beyond. ID3

Digital We (2015) *Eigen Data Delen.* Beschikbaar via https://innovalor.nl/expertises/digital/publicaties-digital-we/.

InnoValor/Newcom (2015). Nederlanders over persoonlijke data. Beschikbaar via: https://innovalor.nl/wp-content/uploads/2016/09/2015-Nederlanders-over-Persoonlijke-Data-V3.7.pdf

InnoValor (2016) *Haalbaarheidsstudie Qiy pilots.* In opdracht van ICTU.

Makaay , Smedinghoff & Thibeau (2017). Trust Frameworks for Identity Systems. Oix whitepaper. Beschikbaar via: https://connectis.nl/nl/blog/trust-frameworks-voor-identity-systems/

MedMij (2017) *Architectuur Afsprakenstelsel* Verkrijgbaar via http://www.medmij.nl/wp-content/uploads/2017/05/20170518-Medmij_Architectuur.pdf

MijnOverheid (2016). MijnOverheid van de toekomst. Beschikbaar via: https://digitaleoverheid.pleio.nl/file/download/44405592

Ministerie van BZK (2012) *NORA 3.0 Principes voor samenwerking en dienstverlening*

MyData (2015) *A Nordic model for human centered personal data management and processing.* Beschikbaar via http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/78439/MyData-nordic-model.pdf?sequence=1

Mydex (2017) *MyDex developer documentation.* Beschikbaar via https://dev.mydex.org/

Privacy Management Partners (2017) *Privacy Impact Assessement Qiy*

Programma Regie op Gegevens (2016) *Persoonlijke Data Management*

Qiy Foundation (2015) *Definitions of the Qiy Scheme v1.0*

Schluss (2017) *Technical overview.*

The Sovrin foundation (2016) *Sovrin: Glossary of terms.*

Bijlage – details van initiatieven en stelsels) zijn verschillende ontwikkelingen in meer detail beschreven. We beperken ons hier tot de hoofdlijnen.

3.1 OPLOSSINGEN

3.1.1 AFAS personal

AFAS Personal is een online huishoudboekje. Je brengt al je geldzaken samen op één plek. Hierdoor heb je overzicht in je inkomsten en uitgaven. AFAS personal komt in een gratis en een betaalde variant (€2,99 per maand), waarbij je uitgaven kunt classificeren en bewaken, kunt budgetteren, spaardoelen kunt invoeren etc. De gegevens worden bewaard op een centrale plaats in een Nederlands datacenter, maar zijn niet toegankelijk voor personeel van AFAS. Er wordt geen informatie gedeeld met derden.

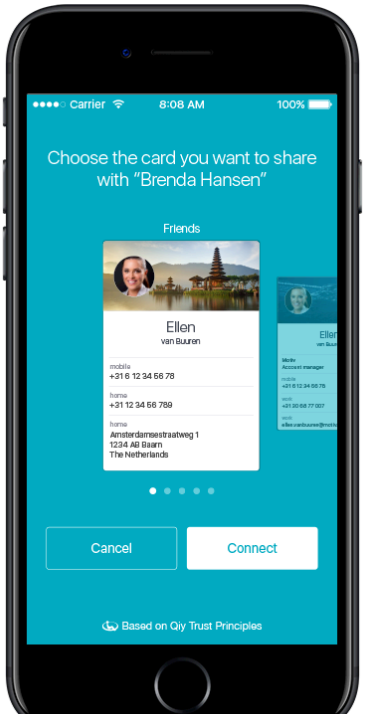
AFAS personal koppelt ook de loonstroken vanuit de AFAS software aan het huishoudboekje als deze beschikbaar zijn. Daarmee gaat het een stap verder dan huishoudboekjes zoals deze soms bij internetbankieren worden geleverd.

3.1.2 CV Monitor

De CV Monitor is een service gericht op het valideren van CV's. Een persoon kan zijn CV uploaden en updaten, afhankelijk van het CV onderdeel kan dit volledig digitaal of via PDF. De documenten worden online geregistreerd in een digitale kluis. Wanneer een werkgever het gecheckte CV van de persoon wil inzien is dat mogelijk tegen betaling. Dit maakt het voor werkgevers mogelijk om de CV's van sollicitanten te verifiëren.

Een CV wordt gecheckt op echtheid met databases van de overheid. Dit gebeurt automatisch wanneer de sollicitant zijn gegevens uploadt in CV monitor. Er wordt namelijk een koppeling gemaakt met overheidsinstanties, bijvoorbeeld DUO voor diploma's, en de gegevens worden opgehaald. Dit proces verloopt via een DigiD autorisatie van de sollicitant. Sommige processen, zoals het aanvragen van een VOG, zijn echter nog niet te digitaliseren.

CV monitor is op dit moment werkend, en kan gebruikt worden door sollicitanten en werkgevers.



Afbeelding 2: Dappre Card

3.1.3 Dappre

Dappre is een app die een deel van het Qiy truststelsel implementeert, waarbij het individu controle heeft over wat hij met wie deelt. In Dappre worden beveiligd attributen uitgewisseld. Op dit moment kan iedereen aanmelden en beginnen met het bewaren en delen van contactgegevens. Dat delen kan zowel tussen personen als met bedrijven. Dappre wordt ontwikkeld door Digital Me, het voldoet dan ook aan de principes van de Qiy Foundation.

Dappre is beschikbaar op iOS en Android en is in verschillende situaties toegepast. Bij Aegon wordt Dappre gebruikt als manier om in te loggen, naast onder meer Facebook en Google. Dit is een vorm van social login, waarbij je identiteit in de Qiy Node, die via Dappre wordt ontsloten, wordt gekoppeld aan je Aegon accounts. In juli 2017 zal ook in de gemeente Boxtel een pilot met Qiy/Dappre live gaan, zo is de verwachting.

Dappre werkt met kaartjes, waarin je verschillende varianten van je identiteitsgegevens kunt bewaren en kunt uitwisselen. Conform het Qiy truststelsel worden kaartjes bijgewerkt als je ze met anderen hebt uitgewisseld. In Dappre gaat nog puur om "self-asserted data", d.w.z. persoonlijke gegevens die je er zelf in stopt. Er is geen relatie met door de overheid of door banken uitgegeven identiteiten zoals via DigiD of iDIN.

Naast uitwisselen van kaartjes kun je ook berichten uitwisselen onderling, ook in groepen (tribes genoemd in Dappre). Dappre is voor consumenten gratis. Bedrijven die gebruik van Dappre willen maken voor hun klanten betalen een vergoeding. Als bedrijven ook informatie willen uitwisselen betalen ze ook een licentie op het Qiy Trust Framework (€20.000 per jaar).

3.1.4 DataPlaza

DataPlaza is een service rond het bewaren van persoonsgegevens met een focus op notariële dossiers. Via een beveiligd platform kan een persoon informatie uitwisselen met notarissen. De notaris kan de informatie

vervolgens valideren voor de ontvangende partij, zoals een makelaar of een hypotheker. Er wordt gewerkt met NotarisID om de identiteit van de Notaris vast te stellen. Dit zorgt ervoor dat er zekerheid is over de identiteit van de notaris die met de gegevens mag werken. De meerwaarde van DataPlaza is dat het de uitwisseling van documenten tussen deze partijen makkelijker maakt, door processen waar de notaris bij betrokken is te digitaliseren.

DataPlaza geeft aan vooral behoefte te hebben aan een gestandaardiseerde manier van berichtenuitwisseling. Daarnaast is er ook behoefte aan een waarborg dat organisaties op een veilige manier omgaan met data. DataPlaza is op dit moment in gebruik om dossiers te bewaren, voorlopig is de functionaliteit als PDM service daarmee beperkt tot 'gegevenskluis'. Koppelingen met andere organisaties zijn momenteel in ontwikkeling. In juli 2017 start een pilot met Makelaarsland. Daarnaast is ook de 'Digitale Erfenis' in ontwikkeling. Deze uitbreiding moet het mogelijk maken voor een persoon om zaken als wachtwoorden en profielen te delen met nabestaanden. Inmiddels wordt er aan DataPlaza gebouwd.

3.1.5 Dime

Dime is een personal data service met het oog op waarde van data teruggeven aan het individu, over wie de data gaan. Personen kiezen zelf wat ze delen, met welke organisatie en krijgen hier geld voor terug. Dime is opgestart in 2016 en is momenteel in ontwikkelfase. Er zijn nog geen implementaties van Dime, hoe dit initiatief zich verder zal ontwikkelen is op dit moment nog niet duidelijk.

3.1.6 Financieel Paspoort

Het idee van Financieel Paspoort is om een app te maken waarin financiële data uit verschillende bronnen bij elkaar wordt gebracht. Het geeft de mogelijkheid om specifieke gegevens te delen, bijvoorbeeld aan financieel adviseurs. Financieel Paspoort is voortgekomen uit jongereninitiatief PensioenLab, met het idee dat iedere burger het recht heeft op een inzichtelijk financieel overzicht, zijn hele leven lang. Het Financieel Paspoort is op dit moment nog in conceptuele fase, het is nog geen service aanbieder.

3.1.7 Cleverbase

Cleverbase ontwikkelt een persoonlijk platform waar zakelijke informatie veilig en overzichtelijk is opgeslagen. Vanuit het platform kunnen burgers en ondernemers documentatie digitaal ondertekenen en op een gestructureerde manier informatie uitwisselen met de overheid, financiële instellingen en het bedrijfsleven. Koppelingen met commerciële softwarepakketten zijn mogelijk. Het platform geeft burgers en ondernemers controle, overzicht en zekerheid over hun zakelijke informatie. Onderdeel van de oplossing van Cleverbase is een betrouwbare authenticatie van de gebruiker middels Idensys en eHerkenning met een hoog betrouwbaarheidsniveau. Cleverbase is ISO27001 gecertificeerd en is voornemens om op korte termijn live te gaan met het platform met toepassingen in de Financiële- en HR-sector.

3.1.8 HealthSuite

De HealthSuite van Philips gaat om het combineren van gezondheidsdata van 'smart devices' met data van zorgverleners. Het is een cloud-based platform, dat open is voor derde partijen en data uit hardware, zoals smartwatches, kan verbinden aan data van zorgverleners. Dit geeft patiënt en behandelaar een compleet beeld van de medische situatie van de patiënt. Zorgverleners kunnen analyses doen over de data van de gehele populatie. HealthSuite werkt met een app en portal met persoonlijke login. Het systeem is op dit moment in ontwikkeling, er loopt een pilot met diabetespatiënten en zorgverleners in samenwerking met Zorgnetwerk Midden-Brabant.

3.1.9 IRMA

"I Reveal My Attributes" is een oplossing die is gericht op het delen van attributen. Alleen de attributen die nodig zijn voor een transactie worden gedeeld, zonder andere informatie te verstrekken. Het werkte initieel met een 'smart card', maar de ontwikkelingen zijn verschoven naar een smartphone applicatie. Dit betekent dan ook dat IRMA focust op het verstrekken van attributen in een digitale wereld, en niet, zoals met de smartcard mogelijk was, bij de slijter op de hoek. Attributen kunnen wel opgehaald worden in de fysieke wereld door een combinatie dataoverdracht via van QR-codes en face-to-face authenticatie. Op dit moment is IRMA nog in ontwikkeling. Er zijn twee pilots geweest in 2015 met Universiteit Twente en Universiteit Nijmegen.

3.1.10 Landelijk Schakelpunt

Wanneer patiënten hiervoor toestemming hebben gegeven, kunnen zorgverleners via het Landelijk Schakelpunt (LSP) medische gegevens bij andere zorgverleners op een veilige en betrouwbare manier inzien, uitsluitend wanneer dit voor de behandeling noodzakelijk is. In het LSP staan het Burger Service Nummer (BSN) en welke aangesloten zorgverleners een bijbehorend medisch dossier beschikbaar hebben. Momenteel zijn alleen huisartsenpraktijken (89%), apothekers (94%), huisartsenposten (96%) en ziekenhuizen (81%) aangesloten op het LSP. Het medisch dossier blijft de verantwoordelijkheid van de zorgverlener en staat niet in het LSP.

Het LSP heeft een mijn-omgeving waarop burgers kunnen inloggen met DigiD om een inzage-overzicht te bekijken van welke zorgverleners welke medische gegevens hebben opgevraagd. Ook biedt de mijn-omgeving gebruikers de mogelijkheid om zich te abonneren op een melding bij inzage van gegevens. Zorgverleners kunnen alleen een vereiste selectie van persoonlijke en medische gegevens inzien. Bovendien kan men in overleg met zorgverleners vragen bepaalde gegevens af te schermen. In wezen fungeert het LSP als een PDS voor het inzien en delen van medische gegevens, maar is hierin beperkt. Zo kunnen gebruikers in het LSP nog niet de eigen medische dossiers inzien.

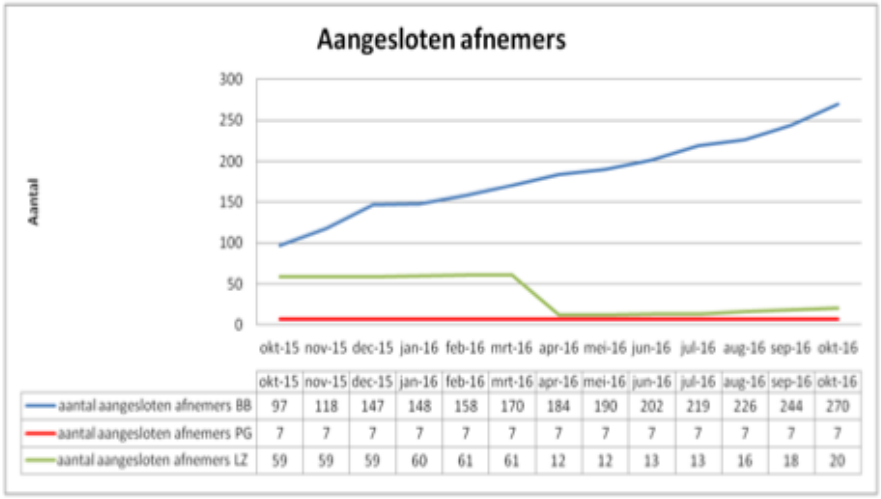
Door verschillende partijen wordt gesproken over een koppeling tussen het Landelijk Schakelpunt en Persoonlijke Gezondsheidsdossiers. Een koppeling met het PGD zou het mogelijk maken om via het LSP de eigen medische informatie in te zien, op te slaan en te kopiëren. Het LSP blijft echter omstreden, vooral om redenen van veiligheid en privacy. Recentelijk presenteerde de Huisartsenkring Amsterdam in samenwerking met de Universiteit van Amsterdam een decentraal alternatief systeem voor het centrale LSP dat een deel van deze zorgen zou kunnen wegnemen.

3.1.11 Leaflad

Leaflad is een personal data service waarbij personen hun 'voorkeuren' kunnen delen met adverteerders. De persoon krijgt 20% van de advertentieopbrengsten die zijn voorkeuren hebben opgebracht. Dit kan vervolgens besteed worden aan producten die door de adverteerders worden aangeboden. Leaflad is opgericht in 2014 en op dit moment in bèta fase. Aanmelden is mogelijk.

3.1.12 Mijn Overheid

MijnOverheid is een combinatie van digitale post (Berichtenbox) en diensten voor de burger vanuit de overheid. Het geeft inzicht in persoonlijke gegevens die de overheid van de burger heeft. MijnOverheid ontsluit via een portaal de zaken die bij een veelheid van instanties lopen, van kinderbijslag bij de SVB, WOZ-waarde bij het kadaster tot gemeentelijke zaken; een personal data service voor burgers. Er is onder meer direct inzicht te krijgen in de data die de basisregistratie personen (BRP) heeft, inkomensgegevens zoals bij de Belastingdienst bekend zijn, woninggegevens van Kadaster en kentekenregistratie van het RDW. Daarnaast wordt er ook naar een aantal andere 'mijn omgevingen' doorgelinkt, waaronder Donorregister, DUO en Pensioenregister. Inmiddels zijn meer dan 270 organisaties aangesloten.



	okt-15	nov-15	dec-15	jan-16	feb-16	mrt-16	apr-16	mei-16	jun-16	jul-16	aug-16	sep-16	okt-16
aantal aangesloten afnemers BB	97	118	147	148	158	170	184	190	202	219	226	244	270
aantal aangesloten afnemers PG	7	7	7	7	7	7	7	7	7	7	7	7	7
aantal aangesloten afnemers LZ	59	59	59	60	61	61	12	12	13	13	16	18	20

Afbeelding 3: Aantal organisaties die aangesloten zijn op MijnOverheid

MijnOverheid ontsluit primair richting de burger, het speelt geen rol in het doorgeven van de gegevens aan derden. Gegevensuitwisseling met derden gebeurt door de achterliggende organisaties zelf op basis van wettelijke gronden, niet via de burger.

Bron	***Verantwoordelijke***	***Koppeling***
1 Persoonsgegevens/BRP	Rijksdienst ID-gegevens	webservice
2 Identiteitsbewijs/IDMS	Rijksdienst ID-gegevens	webservice
3 Kadastraal eigendom	Kadaster	webservice
4 Voertuig/kenteken	RDW	webservice
5 Digitaal Klant Dossier W&I	UWV/BKWI	webservice/portlet
6 Inningsdata 'alimentatie'	LBIO	webservice
7 WOZ & taxatierapporten	gemeenten	webservice
8 Authentiek Inkomen	Belastingdienst	webservice
9 Diplomaregister	*DUO (vjr 2017 verwacht)*	*webservice*
Donorregister	CIBG	hyperlink
MijnDuo	DUO	hyperlink
MijnSVB	SVB	hyperlink
MijnPensioenregister	St.Pensioenregister	hyperlink+SSO
Verzekeringsgegevens	UWV	hyperlink
MijnToeslagen	BD	hyperlink
MijnBelastingdienst	BD	hyperlink

Afbeelding 4: Overzicht ontsloten bronnen MijnOverheid (eind 2016).

Inloggen bij Mijn Overheid gebeurt via DigiD. Sinds oktober 2015 is het gebruik van MijnOverheid voor burgers vanaf 14 jaar verplicht. Op dit moment (2017) wordt de BerichtenBox uitgebreid waardoor binnenkort grotere berichten verwerkt kunnen worden.

3.1.13 MijnPensioenoverzicht

MijnPensioenoverzicht is een personal data service die alle pensioen polissen van een persoon bij elkaar brengt. Dit initiatief is ontwikkeld in 2008, omdat wetgeving vroeg om een overzicht van pensioeninkomsten van burgers. Het is op dit moment bruikbaar en het is voor alle pensioenaanbieders verplicht om aan te sluiten. Het is daarnaast ook bereikbaar via MijnOverheid. Belangrijk hierin was de standaardisatie via het Uniform Pensioenoverzicht, waar door informatie uit verschillende bronnen combineerbaar is.

3.1.14 The Moneyer

The Moneyer is een dienst rond financiële data van een individu: personal finance management. The Moneyer is een Nederlandse organisatie, gevestigd in Amsterdam. The Moneyer is opgericht in 2011 en is op dit moment voor consumenten bruikbaar. De kern van Moneyer is het bij elkaar brengen van de financiële gegevens van diverse bankrekeningen. Dit wordt vervolgens versleuteld en geanonimiseerd opgeslagen op een beveiligde Zwitserse server. Hier kan The Moneyer vervolgens analyses op doen en kijken naar zaken als bestedingspatronen. Het is o.a. mogelijk om financiële doelen te stellen en een persoonlijke financieel plan te koppelen aan de data. De gebruiker kan daarnaast zelf bepalen of hij/zij dit wil delen met andere service aanbieders.

The Moneyer wordt ook door banken gebruikt, voornamelijk nog in het buitenland. Met de komst van PSD2 krijgt personal finance management een steviger fundament met meer mogelijkheden.

Afbeelding 5: De Ockto app

3.1.15 Ockto

Ockto is een service die gegevens kan verzamelen van Belastingdienst, UWV en Pensioenoverzicht. Het laat de financiële data van deze sites zien, in een overzicht in de Ockto app. Dit overzicht kunnen vervolgens gedownload en gedeeld worden. De gegevens worden niet bewaard door Ockto, als je de app sluit is de data weg.

3.1.16 Only Once

Only Once is opgericht in 2013, nadat het bedrijf €900.000,- aan crowdfunding had opgehaald. De Only Once service moet het makkelijker te maken om

attributen zoals contactinformatie uit te wisselen en up to date te houden. De service is bereikbaar via een applicatie op smartphones. Via een persoonlijk adresboek wordt informatie over contacten verzameld. Gebruikers kunnen daarin zelf bepalen welke informatie ze delen, en welke informatie publiek opgevraagd mag worden. De contactinformatie kan via 'kaartjes' gedeeld worden. Only Once is op dit moment bruikbaar en richt zich met name op personen en organisaties die met regelmaat zakelijke gegevens uitwisselen.

3.1.17 Poliskluis

Het Verbond van Verzekeraars is in 2014 begonnen met het de ontwikkeling van de poliskluis. De ontwikkeling van poliskluis is gestart nadat uit onderzoek van de consumentenbond duidelijk werd dat mensen behoefte hadden aan overzicht in hun verzekeringen. Dit is dan ook wat de poliskluis biedt. Het initiatief is vergelijkbaar met mijnpensioenoverzicht en zorgt ervoor dat personen niet langer op meerdere plaatsen moeten zoeken, om een overzicht te hebben van lopende verzekeringen.

Het lastige in de ontwikkeling van Poliskluis, was dat BSN niet zomaar gebruikt kon worden om te verzekeringen te kunnen koppelen aan de persoon. In eerste instantie werd gewerkt met een koppelregister, maar inmiddels worden iDeal en iDIN hiervoor ingezet.

Het verzekeringsoverzicht is te bekijken op mijnverzekeringenopeenrij.nl. De informatie op mijnverzekeringenopeenrij wordt beveiligd bewaard en is te delen met anderen. De website is op dit moment nog in ontwikkeling, verzekeraars worden nu aangesloten en naar verwachting eind 2017 komt het beschikbaar voor gebruikers.

3.1.18 Schluss

Schluss is een service rond het bewaren van persoonsgegevens, waarbij de gebruiker controle heeft over wat hij deelt met wie. De toegevoegde waarde van Schluss is dat de gebruiker zelf regie heeft over de data die hij via Schluss uitwisselt, op een veilige manier. De visie hierachter is dat alleen jij mag bepalen wie wat van je weet en dat de datastroom moet worden omgedraaid. In de kern gaat het om beveiligd attributen uitwisselen. Dat moet zelfs anoniem kunnen, dus met een pseudoniem. Schluss volgt daarmee de benadering van een datakluis.

Samengevat is Schluss een interessant nieuw initiatief vanuit een maatschappelijk belang van PDM. De coöperatieve structuur met een eenvoudig verdienmodel is daarin een nieuw element ten opzichte van andere ontwikkelingen. Ook het streven naar open source implementaties is onderscheidend. Technisch staat Schluss nog in de kinderschoenen. De komende pilots moeten hier verdere invulling aan geven.

3.1.19 Social JO!N

Social JO!N biedt een generiek en op open source standaarden gebaseerd digitaal platform dat communiceren, informeren en samenwerken in samenhang ondersteunt. Een platform dat het individu, vanuit haar verschillende rollen, centraal stelt in haar interactie met organisaties en professionals binnen het sociaal domein en de (lokale) overheid. Social JO!N is een initiatief van Thorax (www.thorax.nl)

Met het platform van Social JO!N streeft men naar een integraal communicatie en samenwerkingsplatform in Twente waar het individu centraal staat en betrokken instanties en overheden op aansluiten om zo een samenhangend en verbindend digitaal kanaal te realiseren. Social JO!N biedt de techniek en werkt aan het realiseren hiervan, samen met een steeds groter wordende groep van partners en overheidsinstanties om de gewenste transformatie te ondersteunen.

3.1.20 Tippiq

Tippiq is een PDM service gericht op woningen. Het idee is om via het Tippiq platform diensten te koppelen aan de woning van een gezin en op basis van de woonplaats relevante informatie te bieden over de buurt. Personen kunnen zelf kiezen welke informatie over hun woning ze delen met de diverse diensten. Op dit moment is Tippiq nog in ontwikkeling, maar al wel bruikbaar voor consumenten. Het is mogelijk om een woning aan te melden, en te zien welke activiteiten er in de buurt van de woning zijn. De ambitie is om meerdere third party diensten aan Tippiq te koppelen.

3.1.21 Ydenti

Ydenti is een service die personen helpt om erachter te komen welke organisaties over persoonlijke gegevens beschikken. Na verificatie van de identiteit van het individu, kan Ydenti helpen bij het uitvoeren van bepaalde

rechten. Zoals het recht van inzage, verzet en vergeten. Personen kunnen bijvoorbeeld automatisch inzageverzoeken en vergeetverzoeken aanvragen. Ydenti biedt daarmee een makkelijke manier om van dit soort rechten gebruik te maken. Daarnaast kan de service ook een verhuizing doorgeven, de persoon kiest hierbij met welke organisaties hij deze gegevens deelt. Ydenti kan op dit moment gebruikt worden.

3.2 AFSPRAKENSTELSELS

3.2.1 Idensys

Idensys is een systeem voor online authenticatie van burgers, zowel bij de overheid als bij private partijen. Het ministerie van Economische Zaken opereert als eigenaar van het Idensys afsprakenstelsel. Idensys biedt plaats voor meerdere aanbieders van authenticatiemiddelen; deze kunnen ook door private partijen verstrekt worden. Dit betekent dat een publieke partij gebruik moet kunnen maken van het BSN om een burger te identificeren, ook als deze inlogt met een middel wat verstrekt is door een partij die zelf het BSN niet mag gebruiken. Hiertoe is het BSN-koppelregister opgezet.

Met één Idensysmiddel kan een gebruiker bij verschillende organisaties inloggen. Maar niet iedere organisatie behoeft hetzelfde betrouwbaarheidsniveau (i.e. Level of Assurance of LoA); daarom zijn de Idensys middelen op verschillende niveaus verkrijgbaar (2 t/m 4). Voor inloggen op niveau 2 is een combinatie van gebruikersnaam en sterk wachtwoord voldoende, op hogere niveaus komt daar een tweede factor bij, zoals een one-time password via sms of het invoeren van een pin in een app. Zo'n tweede factor kan verschillen per aanbieder; ook hier heeft de gebruiker dus de keuze.

Er zijn momenteel vier aanbieders van Idensys middelen, en er kan bij zo'n 20 partijen met Idensys ingelogd worden: o.a. de belastingdienst, verschillende gemeenten, zorgorganisaties en enkele private organisaties.

3.2.2 iDIN

iDIN is een authenticatiesysteem ontwikkeld door Nederlandse banken. Klanten van banken kunnen ermee inloggen bij overheidsinstanties en private partijen. Daarvoor gebruiken ze dezelfde inlogmiddelen die zij ook voor online bankieren gebruiken. iDIN lijkt qua gebruikersinteractie op het veel gebruikte iDEAL; maar in plaats van na het inloggen een financiële transactie te doen, vind er een transactie plaats van attributen die de dienstaanbieder vraagt.

Het afsprakenstelsel rondom iDIN wordt beheerd door de Betaalvereniging Nederland. Zeven verschillende banken fungeren momenteel als zogenoemde 'issuer' van het inlogmiddel. Momenteel is het mogelijk om bij zo'n tien verschillende organisaties in te loggen met iDIN; o.a. de belastingdienst, maar ook private partijen zoals verzekeraars.

Zowel iDIN als Idensys kunnen dus bij overheidsinstellingen gebruikt worden voor authenticatie. Daarnaast bestaat ook DigiD nog steeds; deze kan alléén bij publieke organisaties gebruikt worden, niet bij private. De onderstaande plaat geeft een overzicht van deze verschillende authenticatiemiddelen.

Afbeelding 6: Samenhang Idensys, iDIN en DigiD

3.2.3 MedMij

MedMij is een afsprakenstelsel dat wordt ontwikkeld door o.a. Nictiz. MedMij is ook een behoeftesteller: Het kaart de noodzaak aan en zet aan tot dialoog rond persoonlijke data vraagstukken in de context van gezondheid. Het afsprakenstelsel is gericht op uitwisseling van zorggegevens. Het moet ervoor zorgen dat privacy geborgd is bij uitwisseling en dat systemen aan juridische eisen voldoen.

Een lastig punt voor het stelsel, is hoe om te gaan met machtigingen tussen burgers. Bijvoorbeeld iemand die vertegenwoordiger is voor een ander, moet bij de medische gegevens kunnen in geval van nood. Daarnaast is het wettelijk kader rond PDM momenteel onduidelijk, hier zou de overheid een rol kunnen spelen.

Het stelsel is volop in ontwikkeling, de eerste juridische kaders zijn in maart 2017 gepubliceerd. Er zijn nog geen implementaties van MedMij. Op dit moment is MedMij op zoek naar partners om pilots mee te doen en die uiteindelijk het stelsel willen implementeren. De eerste pilots starten in de zomer.

3.2.4 Qiy Afsprakenselsel

Het afsprakenstelsel Qiy biedt individuen de mogelijkheid persoonsgebonden gegevens uit te wisselen met het publieke en private domein. Gegevensuitwisseling vindt plaats onder regie van de burger, de burger is de centrale spil. Daartoe bevat de persoonlijke Qiy Node, van waaruit gegevens worden uitgewisseld, verwijzingen naar persoonlijke gegevens. De Qiy Node bevat zelf praktisch geen gegevens; de Qiy Node is dus geen traditionele kluis. Het uitwisselen van gegevens via de persoonlijke Qiy Node gebeurt doordat de burger via zijn Qiy Node partij A laat antwoorden op een vraag/vragen van partij B. Het antwoord is beschikbaar gedurende een van tevoren bepaalde termijn.

Het afsprakenstelsel Qiy betreft niet de inhoud en semantiek van uitgewisselde gegevens. Qiy maakt het mogelijk ‘gesloten enveloppen’ te routeren. Een partij die bij de routering van dergelijke ‘gesloten enveloppen’ betrokken is kan niet verder kijken dan de eerste eerder en de eerste latere partij in de routeringsketen. Dit betekent dat bestaande informatiemodellen en standaarden kunnen worden gebruikt. Daarnaast maakt Qiy gebruik van diensten voor verificatie van de identiteit en bijbehorende gegevens. Identificatie en authenticatie is geen onderdeel van Qiy zelf.

Het afsprakenstelsel Qiy gaat uit van een aantal principes, dat de rechten van het individu omschrijft wanneer deze gegevens uitwisselt via het Qiy Trust Framework. Alle actoren binnen het afsprakenstelsel moeten zich aan deze regels houden.

Het stelsel is nog in volop in ontwikkeling, er zijn wel een groot aantal partners betrokken bij het stelsel die in de ontwikkeling ervan investeren. De governance laag is definitief en publiek beschikbaar. De onderliggende schemes en technologie zijn nog niet volledig uitgewerkt en nog in ontwikkeling. Deze zijn ook niet publiek beschikbaar.

3.2.5 Trusttester

TrustTester is een trust framework van onderzoeksinstituut TNO. Het afsprakenstelsel is gericht op het valideren van gegevens, die personen zelf invoeren (de zogeheten “self-asserted data”). Het stelsel is gecombineerd met een algoritme dat valideert of de gegevens juist zijn, zonder daadwerkelijk de gegevens te verstrekken. Op dit moment is dit initiatief nog in ontwikkeling. Er zijn nog geen implementaties van. De technische ontwikkeling start in 2017 en TrustTester is op zoek naar partners om de eerste versie mee te piloten.

3.2.6 UETP

Het Unified Economic Transaction Protocol (UETP) is een trust framework, dat is gericht op het standaardiseren van economische transacties. Het wordt ontwikkeld door FOCAFET (Floris Kleemans). Er zijn, voor zover bekend, nog geen implementaties van UETP. Ook TNO en de topsector logistiek investeren substantieel in de ontwikkeling en toepassing van UETP. De exacte status is echter niet duidelijk.

3.3 INTERNATIONAAL

Nederland is zeker niet de enige plaats waar personal datamanagement interesse heeft. Internationaal wordt er zeker zo lang gepionierd met PDM-oplossingen en –frameworks. Ook hier geldt dat er nog geen grote doorbraken zijn, en zelfs een aantal initiatieven is weggevallen. Van het overzicht in Digital We (2015) zijn ontwikkelingen als personal.com al verdwenen en leidt een initiatief als datacoup, waar je je data verkoopt vergelijkbaar met het concept Dime, een marginaal bestaan.

We concentreren ons hier dan ook op een paar grotere ontwikkelingen en een specifiek belang of redelijke mate van succes. Estland is op dit moment een digitaal gidsland en heeft daarin ook elementen van PDM. MyData is een sterke ontwikkeling in Finland en Mydata is een Britse ontwikkeling die al meer dan 10 jaar aan de weg timmert.

3.3.1 E-Estonia

Estland is een volwassen digitale informatiemaatschappij, daarom ook e-Estonia genoemd. Digitale beschikbaarheid van publiek en private diensten is de standaard; in e-Estonia zijn 99% van de overheidsdiensten online. Deze digitale maatschappij is enerzijds gebouwd op principes en wetgeving die innovatie en digitaal burgerschap stimuleren, anderzijds maakt een goede digitale infrastructuur zulke ambities mogelijk. Zo kan met X-road allerlei soorten data veilig en makkelijk worden uitgewisseld, in de publieke en private sector. Een gedegen systeem van digitale identiteiten maakt digitaal burgerschap mogelijk. De kern hiervan wordt gevormd door de ID-card, een smartcard die als fysiek én digitaal identiteitsbewijs dient.

3.3.2 MyData

MyData is een Fins kennisplatform rond PDM waar onderzoekers en organisaties bij aangesloten zijn. Het is in de eerste plaats een behoeftesteller. Door MyData wordt in 2017 voor de tweede keer een PDM conferentie georganiseerd. Daarnaast zijn er meerdere werkgroepen rond MyData en de ambitie bestaat om een open infrastructuur neer te zetten voor personal data services. Deze moet generiek worden over sectoren en internationaal bruikbaar zijn en via API’s te benaderen. De MyData infrastructuur bevat zelf geen data, maar organisaties kunnen erop aansluiten. Personen krijgen daarbinnen de mogelijkheid om consent te geven of en welke data uitgewisseld mag worden.

3.3.3 MyDex

MyDex is een personal data service die erop gericht is om data veilig te bewaren en delen. MyDex is opgericht in 2007, door een aantal investeerders. Het is neergezet als stichting, om te voorkomen dat winst een te grote rol zou spelen. MyDex is op het moment bruikbaar voor consumenten, er kunnen contactgegevens

uitgewisseld worden. Het platform is nog in ontwikkeling: de ambitie is om andere attribute providers te koppelen aan het systeem. Dit initiatief is vooral gericht op de markt in Groot-Britannië.

MyDex is een interessant internationaal initiatief omdat er een uitgebreide omgeving gebouwd is waaraan externe partijen gekoppeld kunnen worden en zich sterk open opstelt, de technische specificaties voor aansluiting zijn bijvoorbeeld vrij gepubliceerd en kunnen als voorbeeld dienen voor andere initiatieven.

3.3.4 openPDS

openPDS is een initiatief van het Massachusetts Institute for Technology (MIT). openPDS biedt een service en framework voor persoonlijke data services. Het zorgt in de basis voor het geanonimiseerd delen van attributen, zonder de uitwisseling van de onderliggende data. De resultaten zijn als open source beschikbaar. Het is primair een research initiatief. Zie Alexandre de Montjoye et al. (2014).

3.3.5 SOVRIN

SOVRIN is een initiatief dat identity management wil regelen via een gedistribueerd grootboek (distributed ledger, oftewel blockchain technologie). Het gedistribueerde grootboek moet het makkelijker maken om PDM oplossingen aan te bieden op een decentrale manier. Het initiatief zorgt ervoor dat geanonimiseerd delen van attributen mogelijk wordt, met consent van degene over wie de data gaat. SOVRIN is een private samenwerking in een non-profit organisatie. Op dit moment wordt er gewerkt aan de implementatie van Plenum, het onderliggende algoritme, en aan het opzetten van nodes waarop de ledger gehost wordt.

SOVRIN is een van de weinige ontwikkelingen in PDS die PDM via blockchain technologie probeert te ontwikkelen. Dit is een interessant onderwerp in onderzoek en zou een oplossing kunnen bieden voor het gevaar van centrale ontsluiting van persoonlijke data. Ook een aantal andere oplossingen kijkt naar blockchain technologie of andere federatieve of decentrale technologie.

4 Status oplossingen en stelsels

4.1 OPLOSSINGEN

De status en focus van de initiatieven in de longlist zijn erg verschillend. Onderstaande matrix geeft een beknopt overzicht van de focus en volwassenheid van de beschreven oplossingen. Al deze oplossingen worden in hoofdstuk 3 nader toegelicht. Bij oplossingen en stelsel die al operationeel zijn geeft het aantal kruisjes een grove indicatie van de mate van adoptie.

Tabel 3: Matrix volwassenheid en focus

Initiatief	*Horizontaal*	*Verticaal*	*Concept*	*Pilot*	*Operationeel*
Dappre	x				x
IRMA	x			X	
Leaflad	x			x	
Only Once	x			x	
Schluss	x			X	
Ydenti	x				x
Cleverbase	X				
AFAS Personal		Financiën			xx
Poliskluis		Verzekeringen			x[3]
CV Monitor		Werving			xx
LSP		Zorg			xxx
Mijn Pensioenoverzicht		Pensioen			xxx
MijnOverheid		Overheid			xxx
The Moneyer		Financiën			xx
Tippiq		Wonen			x
DataPlaza		Wonen		x	
HealthSuite (Philips)		Zorg		x	
Ockto		Financiën		x	
Social JO!N		Sociaal domein		x	
Dime		Advertenties	x		
Financieel paspoort		Financiën	x		

De horizontale (generieke) services Dappre, Only Once en Schluss, werken op dit moment met contactgegevens. Er worden nog geen koppelingen gemaakt met data van andere organisaties. Dit is wel de ambitie van de initiatieven. De data waar organisaties over beschikken zal via koppelingen zichtbaar en aanpasbaar worden voor het individu.

The Moneyer en Tippiq zijn voor de burger bruikbaar en leveren PDM-oplossingen. Moneyer richt zich op financiele data, Tippiq op data met betrekking op woningen. CV monitor maakt het voor sollicitanten mogelijk

[3] Verzekeraars worden nu aangesloten. Eind 2017 beschikbaar voor consumenten

om CV's in te dienen en, onder toestemming, te laten checken op echtheid. Waarna werkgevers het CV van de sollicitant kunnen verifiëren via CV monitor.

Twee van de oplossingen, Dime en Leaflad, zijn primair gericht op het teruggeven van de waarde van data aan personen. Dime geeft de mogelijkheid om gegevens te delen met organisaties, in ruil voor een bepaald bedrag dat naar het individu gaat. Leaflad laat personen hun 'voorkeuren' delen, in ruil voor korting op geadverteerde producten.

MijnOverheid heeft de meeste gerealiseerde koppelingen. Van inkomensgegevens, tot burgerlijke staat en voorkeuren voor donorschap. Echter kan maar een klein deel van de gegevens die op MijnOverheid inzichtelijk zijn, bewerkt of gedeeld worden. Er moet geregeld een uitstap gemaakt worden naar de uitvoerder om data in te zien of aan te passen.

Opvallend is dat

- de meeste services nog in ontwikkeling zijn, in pilot fase zijn, of zoeken naar pilot partners.
- de services die operationeel zijn, zijn allemaal niche oplossingen.
- Veel van de services gegevens op één plek bewaren en willen fungeren als "kluis".

4.2 FRAMEWORKS

In het vorige hoofdstuk hebben we ook een aantal frameworks op een rij gezet.

Tabel 4: Volwassenheid en focus afsprakenstelsels

Afsprakenstelsel	*Horizontaal*	*Vertikaal*	*Concept*	*Toegepast*	*Brede adoptie*
Qiy Foundation	x			x	
TrustTester	x		x		
Idensys		Identiteit			x
iDIN		Banken			x
MedMij		Zorg		x	
UETP		Transacties	x		

Van Qiy en MedMij zijn de eerste kaders gepubliceerd en beschikbaar. Beide zijn bezig met pilots om de frameworks door te ontwikkelen. TrustTester is nog in ontwikkeling en op dit moment op zoek naar pilot partners om het stelsel verder uit te werken.

5 Observaties

De vraag is nu welke lessen we kunnen trekken uit de verschillende initiatieven. Is er een relatie te leggen tussen de aard van het initiatief en het succes of het tempo van uitrol? In de gesprekken bij het inventariseren van de oplossingen is een aantal punten naar voren gekomen, sommigen ook meerdere malen. Dit zijn dus sterk *kwalitatieve* observaties, niet normatieve (algemeen geldende) observaties.

First mover advantage?

In elk geval kun je stellen dat de eerste initiatieven last hebben (gehad) van het moment van introductie. MijnOverheid en Qiy waren vroeg. Hyves is in 2004 opgericht en stond nog in de kinderschoenen. Facebook en Linkedin bestonden al maar waren in Nederland nog onbekend. Data delen was een nieuw fenomeen. Smartphones bestonden nog niet. In dat tijdgewricht liepen ze ver voor de troepen uit. Nieuwere partijen kunnen dan profiteren van de eerdere ervaringen. Ook Mydex was te vroeg voor een doorbraak en ziet pas nu een sterk groeiende adoptie opkomen. Je hebt geen “first mover advantage”, maar juist een “second mover advantage”.

Afbeelding 7: Aantal PDM ontwikkelingen in tijds- en technologieperspectief.

Bedrijfsmodel

Een tweede aandachtspunt is een sluitend bedrijfsmodel. Hoe financier je een ontwikkeling? Veel van de goedlopende initiatieven hebben een eenvoudig model, bijvoorbeeld gefinancierd door een collectief of de overheid (pensioenoverzicht, poliskluis) of vanuit een zakelijke dienst (CV Monitor, The Moneyer). Zonder een duurzaam bedrijfsmodel is het moeilijk om tot een doorbraak te komen. Daarbij kan het bedrijfsmodel in de ontwikkelfase anders zijn dan in de opschaling, maar het moet wel helder zijn, juist ook voor de gebruiker. Een partij als Schluss heeft daarom van meet af aan het bedrijfsmodel meegenomen in het ontwerp op een transparante wijze, waarbij ook de gebruiker een (zo klein mogelijke) vergoeding betaalt. In de ontwikkelfase is een heel ander bedrijfsmodel nodig, waar de investeringen groot zijn bij een klein aantal gebruikers.

Transparantie en vertrouwen

Daarnaast spelen transparantie en vertrouwen een grote rol. Gegeven dat het om persoonlijke data gaat is vertrouwen een belangrijk goed. Hoe generieker de oplossing, hoe meer vertrouwen nodig is. Een specifieke oplossing in een smal domein kan toe met een beperktere vertrouwensbasis. Transparantie geldt zowel voor de inhoud als voor het achterliggende governance en bedrijfsmodel. Dit zou kunnen pleiten voor een open

standaard / open kennis model voor de PDM oplossing. Dit kan echter bijten met een mogelijk verdienmodel. In een scheme als Mydex zijn alle afspraken en standaarden open, maar is de oplossing geen open source. Wel is de oplossing en het stelsel ondergebracht in een not-for-profit organisatie, met heldere uitgangspunten.

Wetgeving als kader

Vertrouwen wordt ook versterkt door wetgeving of een goed kader. Het pensioenregister heeft een wettelijke basis, Idensys heeft een helder kader, MijnOverheid krijgt dit met de GDI ook in sterkere mate. Soms lijkt wetgeving in eerste instantie een ontwikkeling te bevorderen, maar liggen risico's in de implementatie. Daar waar de GDPR direct geldig is in alle lidstaten, zijn in de uitwerking van de PSD2 de nodige verzwakkingen opgetreden die de oorspronkelijke doelen in de weg staan. Een overheid moet daarin stevig in haar schoenen staan en weten welke visie op PDM of e-dienstverlening in het algemeen zij voor staat. De wetgeving rond elektronische gegevensuitwisseling in de zorg (Cliëntenrechten bij elektronische verwerking van gegevens) die in 2016 door de Eerste Kamer is aangenomen[4] is ook een voorbeeld van een wet die de positie van de burger rond zijn of haar gegevens versterkt.

Standaardisatie

Een lichtere rol voor de overheid, of voor branche-organisaties, ligt in de standaardisatie van gegevens. De zorg is daarin ver (HL7 e.a.) en standaardisatie was essentieel in het uniform pensioenoverzicht. Zonder standaardisatie is uitwisseling van gegevens moeilijk: de betekenis ontbreekt. Dit is nadrukkelijk een probleem in de meer generieke stelsels. Met de genericiteit verdwijnt de betekenis. Bij MedMij is standaardisatie een mogelijke succesfactor. Bij sterk generieke stelsels is het moeilijk om tot relevante standaardisatie te komen. Deze zal of heel generieke zijn (puur op koppelvlakken, of semantisch abstract), of te breed waardoor het niet haalbaar wordt. Omgaan met betekenis in een generiek stelsel een serieus dilemma.

Ook standaardisatie van diensten is een aandachtspunt. In de UK is recent een marktplaats voor digitale diensten[5] ontwikkeld, waardoor gevalideerde diensten in een vast format worden ontsloten. Dit kan de adoptie sterk versnellen. Het verdient aanbeveling na te gaan welke rol dit in Nederland zou kunnen spelen.

De rol van een digitale identiteit

Een andere factor die uitrol in de weg heeft gestaan is een goede identiteitsprovider. DigiD bestaat al lang, maar toepassingen beperken zich tot het BSN-domein. Dit leidde tot een wildgroei aan toegangscodes voor elke MijnOmgeving waar je gebruik van wilde maken, van je pensioen tot je verzekeraar en je energieleverancier. Met social login (gebruik van Facebook, Linkedin e.a.) wordt dit hiaat ingevuld voor risico-arme toepassingen die beperkt persoonsgegevens gebruiken. Hiervoor is de standaard Oauth2.0 beschikbaar en breed geadopteerd. iDIN kan in private toepassingen een rol gaan spelen en Idensys middelen en hoger niveau DigiD zal toepassingen met gevoeligere persoonsgegevens gaan faciliteren. We groeien naar een situatie van "bring your own ID" – je kiest zelf met welk middel je in welke situatie je bekendmaakt.

Experimenteerruimte

Binnen de overheid is er weinig ruimte om te experimenteren, zowel technisch als organisatorisch. Dit maakt het moeilijk om nieuwe technologie en toepassingen te introduceren als ze koppelen aan de overheid. Veranderingen wil je niet direct in operationele systemen invoeren. Ook financiering van innovatie binnen de overheid, waar druk op kosten toch al hoog is en de kostenmodellen van generieke diensten ter discussie staan, is moeilijk.

Samenvattend zien we dat specifiekere oplossingen, gesteund door open standaarden of domeinstandaarden, met een transparant doel en bedrijfsmodel op dit moment de beste papieren in huis hebben. Start bij een (domeinspecifieke) vraag en voeg waarde toe, geef ruimte aan experimenten. Maar baseer dat op een infrastructuur die vertrouwen versterkt, met een goede wettelijke basis.

---

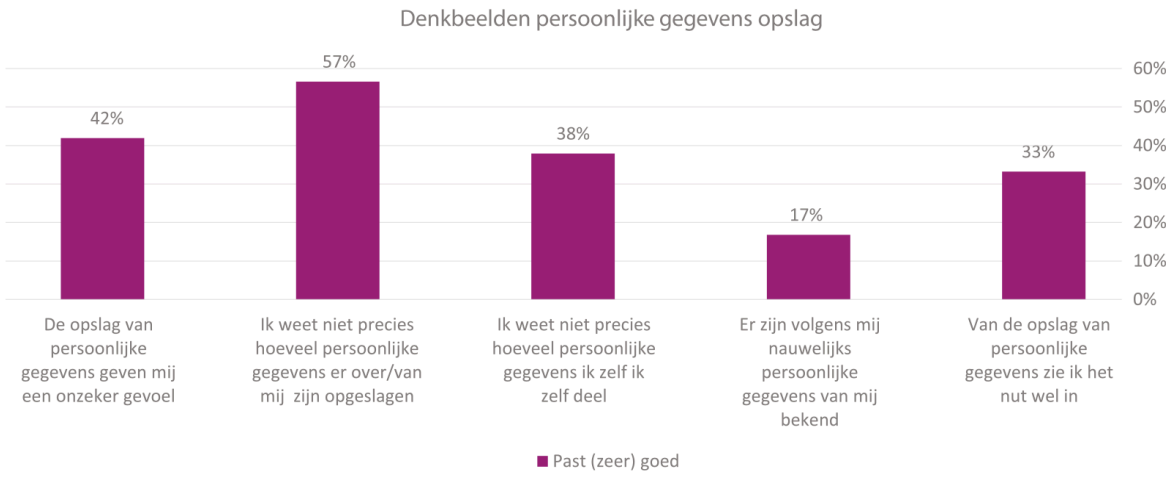
[4] https://www.eerstekamer.nl/wetsvoorstel/33509_clientenrechten_bij

[5] https://www.digitalmarketplace.service.gov.uk/

6 Behoeften van Nederlanders

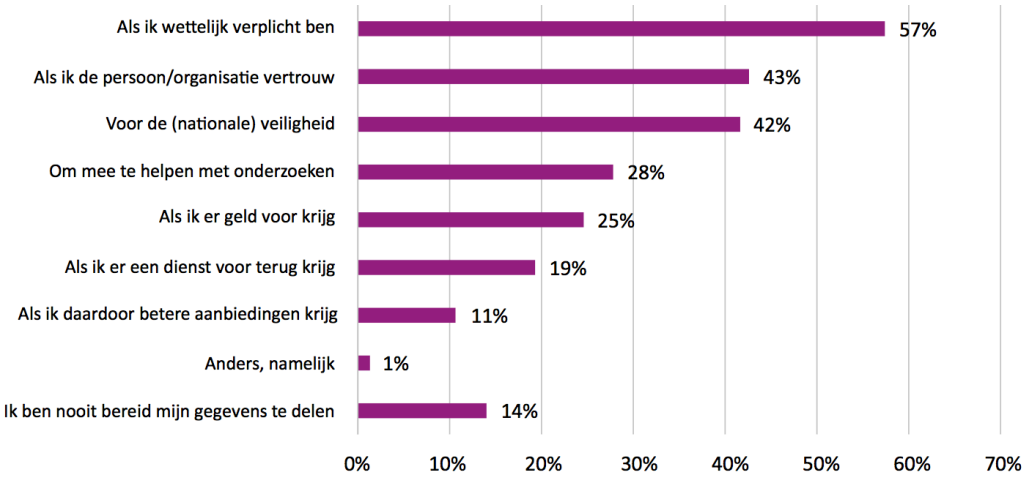
De oplossingen en afsprakenstelsels rond PDM moeten personen en ondernemers helpen om betere regie over eigen gegevens te krijgen. Maar welke behoeftes heeft men op dit gebied? En ziet Nederland de noodzaak hier eigenlijk wel van in? In dit hoofdstuk wordt de mening van Nederlanders beschreven over gebruik en delen van persoonlijke data door en met organisaties. Het onderzoek waar dit hoofdstuk op is gebaseerd is in juni 2015 uitgevoerd door Newcom Research, in opdracht van InnoValor.

Nederlanders blijken wat onzeker als het aankomt op persoonlijke data. Een meerderheid van de respondenten (57%) geeft bijvoorbeeld aan dat ze niet precies weten hoeveel gegevens er over ze zijn opgeslagen. 38% weet ook niet hoeveel ze zelf delen. Het is ook niet duidelijk waarom gegevens opgeslagen worden; twee derde van de mensen ziet het nut niet in van de opslag van gegevens.



Afbeelding 8: Verschillende uitspraken over persoonlijke data, en de hoeveelheid respondenten die aangeeft dat die uitspraak goed bij zijn zijn/haar situatie past

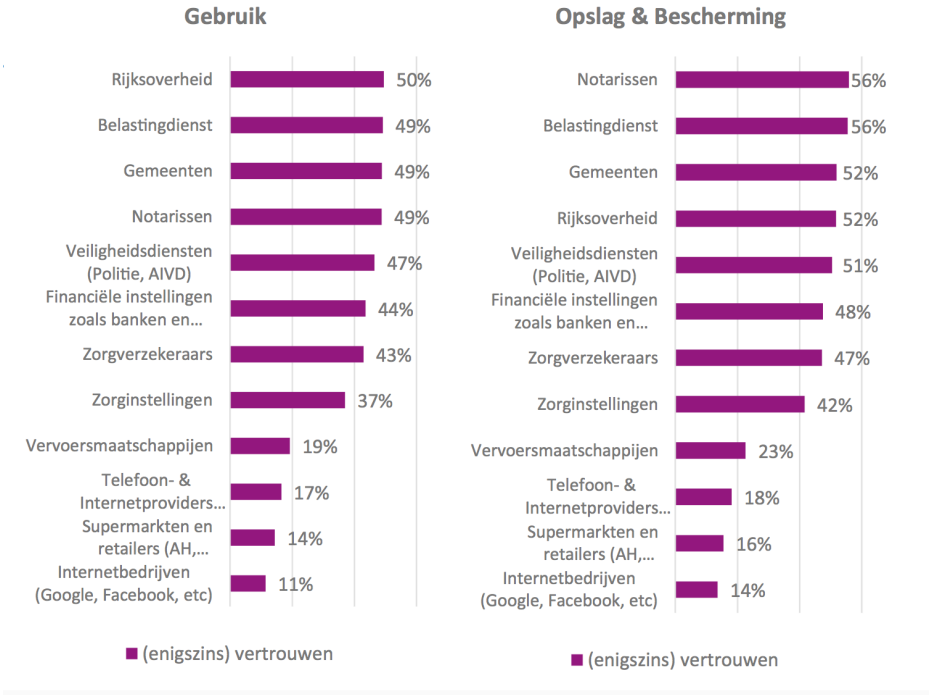
Toch delen we geregeld e-mailadressen op allerlei plaatsen. Dit kan hele verschillende redenen hebben, van korting tot toegang tot gebruik maken van diensten. Soms hebben we dit niet eens door, denk aan het delen van locatie, om een GPS service als Google Maps te kunnen gebruiken. Of het gebruik van de bonus kaart van de AH. Welke derde partijen hier toegang toe krijgen is voor gebruikers meestal onduidelijk. Opvallend is dan ook dat slechts 25% van de respondenten dat ze voor geld persoonlijke data zouden weggeven en maar 19% zegt dit te willen doen voor diensten. Het lijkt er dus op dat personen zich niet realiseren dat ze al persoonlijke gegevens delen in ruil voor deze zaken. Men zegt eerder geneigd te zijn gegevens te delen als dit moet vanwege wetgeving (57%) en wanneer er vertrouwen is in een organisatie (43%).



Afbeelding 9: Verschillende antwoorden op de vraag "Wanneer bent u bereid uw gegevens te delen?"

Maar wie vertrouwen we dan? Wanneer we vragen wie we vertrouwen met opslag en gebruik van onze gegevens komt de overheid positief naar voren (tussen de 56% en 52% vertrouwen). Dit is interessant in het geval van PDM services, mogelijk kan de overheid hier dus een bepalende rol in spelen. Bijvoorbeeld door samen te werken met services, denk aan de koppeling met CV monitor waar dit al gebeurd.

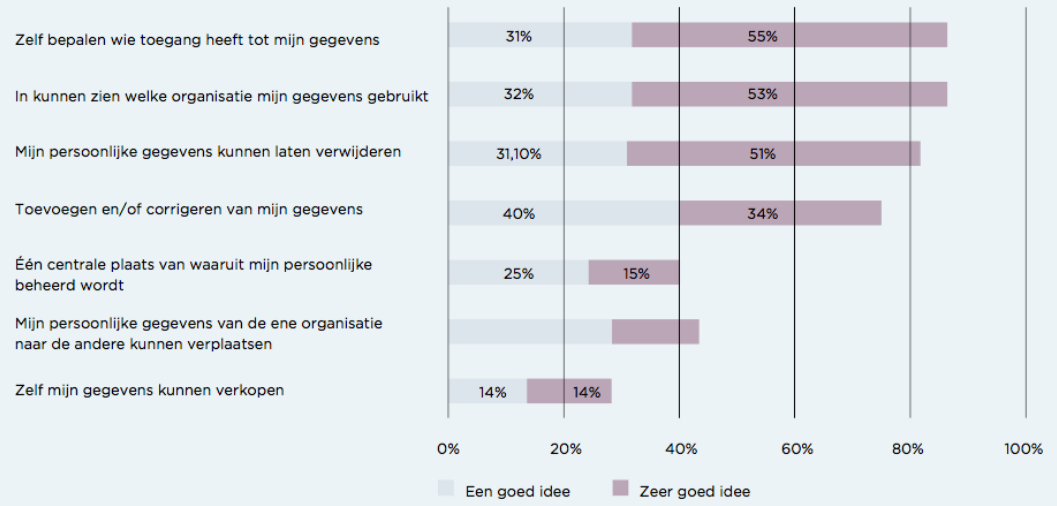
Verzekeraars en zorgverzekeraars en banken worden minder vertrouwd (tussen de 48% en 40% vertrouwen). De introductiestrategie van bijvoorbeeld de Poliskluis, zal transparant moeten zijn en laten zien dat de dienst meerwaarde kan bieden om gebruikers te verleiden tot gebruik ervan. De Internet Service Providers, TelCo's, retail en internetbedrijven(Google, Facebook) scoren overduidelijk slecht.



Afbeelding 10: Welke organisaties worden vertrouwd met het gebruik van data, en welke met de opslag en bescherming ervan?

Toch zegt 57% van de mensen dat ze gebruik zouden maken van een dienst om persoonlijke gegevens te beheren. Mensen willen zelf kunnen sturen: er is een grote behoefte om zelf te kunnen bepalen wie er toegang heeft tot gegevens. Er is een behoefte om controle te hebben. Men wil gegevens kunnen bewerken en kunnen

verwijderen. Dit lijkt te ontstaan uit het gevoel van onzekerheid over wat er met persoonlijke data gebeurt. Er is dus wel degelijk behoefte voor een vorm van PDM. De vraag is dus niet zo zeer of er ruimte is voor Personal Data Management, maar op welke manier het gerealiseerd zal worden.



Afbeelding 11: behoeften rondom persoonlijke data

7 Conclusies

Het thema “persoonlijk data management” speelt al jaren. Na een initiële periode waarin het met name bij voorlopers binnen de overheid en daarbuiten aandacht kreeg (Persoonlijk Internetpagina, MijnOverheid, MijnDenHaag, Qiy) zijn we nu in een periode gekomen waar een veelheid van initiatieven opkomt. Daarvoor zijn verschillende aanleidingen:

- **Maatschappelijk**: er is een groeiend bewustzijn bij consumenten/burgers over de waarde van persoonlijke data. Dit leidt enerzijds tot versterkte aandacht voor privacy en anderzijds tot een groeiende behoefte tot het delen van data waar dat waarde oplevert: in de financiële sector, rond zorg, in relatie tot de overheid.
- **Technologisch**: we verzamelen steeds meer dat zelf, via wearables en smartphones. Die informatie willen we ook kunnen gebruiken. Meerdere dienstenaanbieders springen op deze wens in, zoals Apple en Philips. Daarnaast ontstaat er via ontwikkelingen als Internet of things ook een andere gegevensstroom. Dit versterkt databewustzijn en de mogelijkheden van persoonlijkere dienstverlening.
- **Juridisch**: de PSD2, de wetgeving rond elektronische gegevensuitwisseling in de zorg zijn beide aanleiding voor nieuwe mogelijkheden voor regie op gegevens, vanuit verschillende invalshoeken. Daarnaast realiseert het Idensys raamwerk, ook in combinatie met de GDI, de mogelijkheid van identificerende diensten in de private sector, “Bring your own identity”. Dit vult het breed geaccepteerde DigiD aan vanuit de private sector. Met iDIN kunnen de banken hierin nu een sterke positie innemen als identity service provider.
  Tenslotte zorgt de AVG ervoor dat er een breed bekende basis voor informatie-uitwisseling en privacy, inclusief eisen aan de dienstverlening.

Vanuit deze ontwikkelingen is het niet vreemd dat er een veelheid aan initiatieven ontstaat. Echter: het realiseren van een zorgvuldige dienst binnen dit thema is uitermate complex. Dat leren we van de aanloop die Qiy nodig heeft en de complexiteit van de discussie rondom MedMij. Een PDM-oplossing vereist een robuuste basis die vertrouwen in het de dienstverlening rechtvaardigt.

Veel van de nieuwe initiatieven gaan ietwat lichtvaardig met dit aspect om. Niet per se vanuit kwader trouw, eerder vanuit een gebrek aan kennis of ervaring op dit vlak. De complexe details komen vaak pas aan de orde als het concept echt wordt toegepast in de praktijk op enige schaal.

Tegelijk is het ook goed om met een frisse blik naar het thema te kijken, met de focus op de meerwaarde voor de consument of burger, en minder gericht op de onmogelijkheden of complexiteit. Vanuit de vraagzijde gestuurd is de slaagkans van initiatieven groter dan vanuit de techniek of de principes gestuurd, zeker in de huidige situatie waar het concept nog grotendeels latent is bij de doelgroep (InnoValor/Newcom 2015). MijnOverheid heeft een dergelijke herijking gedaan met haar toekomstscenario’s (MijnOverheid 2016), waarbij de keuzes die daaruit zouden moeten volgen nog niet echt zijn gemaakt. In die zin zijn initiatieven als Schluss en Moneyer alleen al de moeite van het volgen waard.

Een echte doorbraak komt dichterbij wanneer initiatieven kunnen worden verbonden en ze niet meer als eilanden functioneren. Nu nog richt iedereen zich op zijn eigen doel en doelgroep en moet ieder voor zich het vertrouwen van de gebruiker winnen. Vertrouwen dat juist zo wezenlijk is bij regie op gegevens. Consumenten kijken daarbij ook naar de overheid, want juist de overheid is nog steeds een factor van belang als het om vertrouwen gaat. Buiten Idensys is de rol van de overheid nog beperkt: MijnOverheid volgt een beperkte groeistrategie qua functionaliteit en gebruikersnut. Qiy Foundation wordt gesteund met begeleiding in pilots, maar nog niet volmondig als stelsel.

Wat momenteel ontbreekt is een solide gemeenschappelijke basis voor personal data services, waar zicht ontstaat op interoperabiliteit, vendor lockin wordt beperkt en toekomstvaste oplossingen mogelijk worden (Clippinger & Bollier, 2014). Een gemeenschappelijke visie op principes, architectuur en toepassingsvormen, inclusief een heldere rol voor de overheid. Die rol kan velerlei zijn: van toezichthouder tot aan eigenaar/initiator, zoals bij het Idensys stelsel. Een beperkte rol zou kunnen bestaan uit het faciliteren van de

totstandkoming van een open basis, door als gebruiker voorop te lopen, vanuit heldere randvoorwaarden aan het fundament. Onafhankelijk van of de overheid een beperkte of een leidende rol gaat spelen, op deze wijze kan een fundament worden gerealiseerd dat stevig is en aan alle eisen vanuit overheid en burgers voldoet en op die manier de markt voor oplossingen versnelt, met verschillende toepassingsvormen en verschillende architecturen die op elkaar aansluiten in het wezen van regie op gegevens. En met een vertrouwensbasis voor consumenten, burgers en dienstverleners!

Essentieel is daarbij niet bij nul te beginnen, maar juist nu de ervaringen en bestaande kennis te benutten, van Qiy Foundation, OpenPDS, MyData, Idensys, Poliskluis, noem maar op. Die kennis is uitermate waardevol en kan samen de benodigde kwaliteit van het fundament bewerkstelligen.

Referenties

Alexandre de Montjoye et al. (2014) openPDS: Protecting the Privacy of Metadata through SafeAnswers. PLOS One, Beschikbaar via: https://doi.org/10.1371/journal.pone.0098790.

Analyse van afsprakenstelsel Qiy (2016) *Rapport van bevindingen*

Clippinger, J.H, & D. Bollier (red.). (2014) From bitcoin to burning man and beyond. ID3

Digital We (2015) *Eigen Data Delen.* Beschikbaar via https://innovalor.nl/expertises/digital/publicaties-digital-we/.

InnoValor/Newcom (2015). Nederlanders over persoonlijke data. Beschikbaar via: https://innovalor.nl/wp-content/uploads/2016/09/2015-Nederlanders-over-Persoonlijke-Data-V3.7.pdf

InnoValor (2016) *Haalbaarheidsstudie Qiy pilots.* In opdracht van ICTU.

Makaay , Smedinghoff & Thibeau (2017). Trust Frameworks for Identity Systems. Oix whitepaper. Beschikbaar via: https://connectis.nl/nl/blog/trust-frameworks-voor-identity-systems/

MedMij (2017) *Architectuur Afsprakenstelsel* Verkrijgbaar via http://www.medmij.nl/wp-content/uploads/2017/05/20170518-Medmij_Architectuur.pdf

MijnOverheid (2016). MijnOverheid van de toekomst. Beschikbaar via: https://digitaleoverheid.pleio.nl/file/download/44405592

Ministerie van BZK (2012) *NORA 3.0 Principes voor samenwerking en dienstverlening*

MyData (2015) *A Nordic model for human centered personal data management and processing.* Beschikbaar via http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/78439/MyData-nordic-model.pdf?sequence=1

Mydex (2017) *MyDex developer documentation.* Beschikbaar via https://dev.mydex.org/

Privacy Management Partners (2017) *Privacy Impact Assessement Qiy*

Programma Regie op Gegevens (2016) *Persoonlijke Data Management*

Qiy Foundation (2015) *Definitions of the Qiy Scheme v1.0*

Schluss (2017) *Technical overview.*

The Sovrin foundation (2016) *Sovrin: Glossary of terms.*

Bijlage – details van initiatieven en stelsels

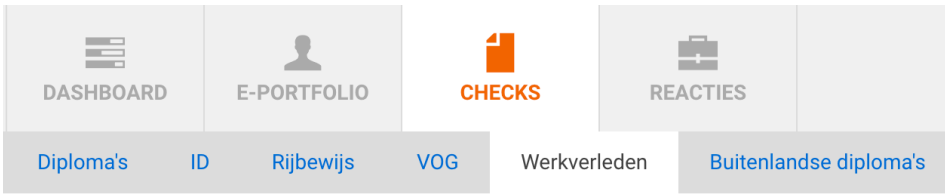
In hoofdstuk 3 zijn alle initiatieven en stelsels kort beschreven. Dit doet niet recht aan de complexiteit van de materie. Van een aantal ontwikkelingen geven we hier ook in meer detail waar ze voor staan. De verschillende ontwikkelingen worden in alfabetische volgorde gepresenteerd.

Dit zijn:

1. CV Monitor
2. DataPlaza
3. E-Estonia
4. Idensys
5. iDIN
6. IRMA
7. Landelijk Schakelpunt
8. MedMij
9. The Moneyer
10. MyData
11. Mydex
12. Only Once
13. Poliskluis
14. Qiy Afsprakenstelsel
15. Schluss
16. Social JO!N
17. Tippiq
18. Ydenti

CV Monitor

CV Monitor is een PDM service rond het checken van CV's. Het initiatief is opgezet door ex-politica Rita Verdonk. Het garandeert betrouwbare cv's door digitale koppelingen met databases van de Overheid. CV monitor levert documenten zoals diploma's, certificaten, identificatiedocumenten, verklaringen en/of bevoegdheidsbewijzen, deze worden online geregistreerd in een persoonlijke digitale kluis.



Afbeelding 12: Dashboard CV monitor

Meerwaarde

CV monitor biedt sollicitanten een alternatief voor het 'steeds opnieuw' handmatig CV's en de daarbij behorende documenten te moeten versturen. Daarnaast worden de CV's gecheckt op echtheid, voor werknemers is het gemakkelijker om de echtheid en correctheid te checken. Diploma gegevens worden bijvoorbeeld opgehaald bij DUO, om dit te realiseren wordt er via DigiD verbinding gemaakt met DUO en worden de gegevens opgehaald. Dit gebeurt met toestemming van de gebruiker, deze moet zijn DigiD gebruiken voor de gegevens kunnen worden uitgewisseld.

Het kan daarnaast zorgen voor massaverwerking van CV's, dit kan voor bijvoorbeeld uitzendbureaus interessant zijn.

Status

CV monitor is op dit moment bruikbaar voor sollicitanten en werkgevers. Het is volledig functioneel met diverse koppelingen naar overheidsinstanties. Sollicitanten kunnen CV's uploaden en werkgevers kunnen CV's van sollicitanten checken. Het is daarmee een van de al verder gevorderde PDM services.

Data en koppelingen

CV monitor is een platform bestaande uit meerdere koppelingen met verschillende overheids-databases. Het voldoet aan de privacy vereisten van de Wet Bescherming Persoonsgegevens (WBP) en is koppelbaar met alle software systemen zowel met rest API als via Website-integratie. De sollicitant kan regie voeren op de eigen persoonsgegevens, de data wordt bewaard.

Ervaringen en succesfactoren

Het succes van CV monitor ligt bij de digitale koppeling met diverse overheidsinstanties. Dit maakt het mogelijk om snel, geverifieerde gegevens te verzamelen. Voor sommige aanvragen kan dit nog steeds een bepaalde tijd in beslag nemen, zoals de aanvraag van een VOG. De data is in bepaalde gevallen ook beperkt geldig, zoals een VOG die maar 3 jaar geldig is. Er zullen dus updates gedaan moeten worden, hiervoor is de sollicitant zelf verantwoordelijk.

Verwachting van de overheid

De overheid is sterk betrokken in CV monitor. De koppelingen en autorisaties via DigiD maken CV monitor feitelijk mogelijk. Zonder deze koppelingen had CV monitor niet in de huidige vorm kunnen bestaan. Verbeteringen zouden gemaakt kunnen worden zodra de overheid eigen processen verder digitaliseert. Bijvoorbeeld in het geval van de aanvraag van een VOG. Hiervoor worden nu nog papieren documenten aangevraagd die gescand moeten worden door de sollicitant.

DataPlaza

Wat biedt DataPlaza?

DataPlaza moet een centraal punt worden voor uitwisseling van gegevens die betrekking hebben op bijvoorbeeld de overdracht van een woning en het afsluiten van een hypotheek. Op dit moment zijn er veel losse koppelingen tussen systemen die hier data over hebben. DataPlaza zorgt ervoor dat consument en notaris maar ook de makelaar en de hypotheekverstrekker een centrale aansluiting hebben waar deze zaken geregeld worden en gegevens uitgewisseld worden.

Het voordeel van DataPlaza is dat het notariaat dat eraan gekoppeld wordt, voor vertrouwen kan zorgen. De notaris is al een bron van vertrouwen bij bijvoorbeeld de aankoop van woning en het verstrekken van een hypotheek. Het idee is dat consumenten consent geven bij het uitwisselen van benodigde data, de notaris garandeert de betrouwbaarheid van de bron van de data die uitgewisseld wordt.

NotarisID, een nieuw identificatiemiddel voor notarissen, zal gebruikt kunnen worden als login voor DataPlaza. Het wordt op dit moment overgedragen aan het KNB. Dit moet een standaardmethode worden om de notarissen te authentiseren.

Wat is de status van DataPlaza?

Op het moment is DataPlaza bruikbaar voor het uitwisselen van online dossiers. Voor de doorontwikkeling en koppeling met derde partijen is een externe software partij ingeschakeld. In juli 2017 zal de eerste koppeling gelegd worden met Makelaarsland.

De vraag hierbij is wel, hoe generiek de koppeling moet zijn die nu gemaakt wordt. Het idee is om met API's te gaan werken, maar voor elke koppeling een andere API is natuurlijk niet de bedoeling, het moet generiek genoeg zijn. Maar gezien in verschillende branches verschillende standaarden gelden zit daar ook een beperking op.

Waar loopt Dataplaza tegenaan in de ontwikkeling?

Waar Dataplaza tegenaan loopt is de soms terughoudende houding van het notariaat, de meerwaarde moet echt bewezen worden. Verder zijn er eigenlijk geen technische hobbels behalve uiteraard de verplichting om het zo veilig als maar mogelijk is op te zetten, volgens de mensen van DataPlaza.

Hoe wordt met bescherming van de data omgegaan?

DataPlaza moet gaan voldoen aan EU regelgeving. De servers waar data bewaard wordt, zullen bijvoorbeeld in Nederland moeten staan. Er zal niet met buitenlandse partners gewerkt worden op dit gebied.

Wat heeft DataPlaza nodig van de overheid?

Opstellen van een gestandaardiseerd berichten uitwisselingsformaat. Er is een norm nodig, met een stuk toezicht daarover (governance). Mogelijk ook een stuk certificering, om te bepalen of een data service voldoet aan die norm. Als deze certificering bestaat, wordt het makkelijker om te bepalen of uitwisseling met bepaalde partners op een veilige manier verloopt.

Mogelijke doorontwikkeling van DataPlaza

Er lopen gesprekken tussen Logius en DataPlaza om de mogelijkheden te bekijken voor koppeling tussen DataPlaza en MijnOverheid. Mogelijk zouden notarissen, via DataPlaza, berichten kunnen sturen naar de berichtenbox van burgers. Zodat afschriften van notariële akten via deze officiële weg gedeeld kunnen worden. Een andere mogelijkheid is een koppeling leggen naar DataPlaza door vanaf MijnOverheid door te linken naar DataPlaza, zoals nu bijvoorbeeld ook bij MijnPensioenoverzicht gebeurt.

e-Estonia

Estland is een volwassen digitale informatiemaatschappij, daarom ook e-Estonia genoemd. Digitale beschikbaarheid van publiek en private diensten is de standaard; in e-Estiona zijn 99% van de overheidsdiensten online. Deze digitale maatschappij is enerzijds gebouwd op principes en wetgeving die innovatie en digitaal burgerschap stimuleren, anderzijds maakt een goede digitale infrastructuur zulke ambities mogelijk. Zo kan met X-road allerlei soorten data veilig en makkelijk worden uitgewisseld, in de publieke en private sector. Een gedegen systeem van digitale identiteiten maakt digitaal burgerschap mogelijk. De kern hiervan wordt gevormd door de ID-card, een smartcard die als fysiek én digitaal identiteitsbewijs dient.

Wat biedt e-Estonia?

Estland is een geavanceerde digitale samenleving; een ware informatiemaatschappij, waarin digitale beschikbaarheid van een groot scala aan diensten, ook die van de overheid, de standaard is. 99% van alle overheidsdiensten in Estland zijn online. Om dit mogelijk te maken voorziet de overheid in één portaal waarin digitale diensten worden aangeboden van verschillende (semi-) overheidsinstellingen. Het is niet alleen mogelijk om alle burgerzaken online te regelen; e-Estiona gaat nog een stap verder.

Zo krijgen burgers en zorgverleners gemakkelijk toegang tot medische dossiers door middel van het e-Health systeem. Dit landelijke systeem integreert medische data vanuit verschillende bronnen tot één elektronisch medisch dossier. De data blijft bij de authoritieve bron, maar zorgverleners kunnen hier toegang tot krijgen. In een noodsituatie bijvoorbeeld kan een zorgverlener met de ID-card van de patiënt toegang krijgen tot de meest essentiële en tijdskritieke medische informatie. Het e-Health systeem lijkt qua werking op ons Landelijk Schakelpunt, maar met een groot verschil: de Estse burger krijgt zélf ook toegang tot zijn medische data via e-Health.

Een van de langstlopende digitale diensten in e-Estonia - begonnen in 1996 - is online bankieren. Door een publiek-private samenwerking tussen banken en de Estse overheid kunnen burgers hun ID-card, uitgegeven door de overheid, gebruiken om veilig online te bankieren.

Een laatste voorbeeld is e-School, een dienst van de overheid waarmee leerlingen en ouders online toegang hebben tot onderwijsgerelateerde informatie. Leerlingen kunnen hun huiswerkopdrachten en cijfers inzien. Docenten en bestuurders kunnen deze onderwijsdata makkelijk administreren en analyseren.

Wat is de status?

e-Estonia is een zeer volwassen digitale maatschappij, die continue in verdere ontwikkeling is. Er zijn drie samenhangende factoren die hier aan bijdragen:

- e-Estonia is gebouwd op principes van innoveren en individuele vrijheid en betrokkenheid. Een van die principes is dat het individu de eigenaar is van zijn persoonlijke data. Ook Estse wetgeving is gericht op innovatie en mag niet belemmerend werken.
- Een ander principe stelt dat de publieke sector de voortrekkersrol vervult in de ontwikkeling van de informatiemaatschappij. Dit blijft niet bij een mooi voornemen op papier maar is al sinds jaar en dag de daadwerkelijke praktijk. Belangrijk hierin is dat de overheid stimuleert, maar niet alles zelf probeert te doen; juist de publiek-private samenwerkingen leiden tot innovatie.
- Om de digitale samenleving te bewerkstellingen is digitale infrastructuur nodig. Ook hier faciliteert de overheid in. Twee belangrijke aspecten van die digitale infrastructuur zijn de uitwisseling van data en de digitale identiteit van burgers.

Architectuur van data-uitwisseling

Data-uitwisseling in e-Estonia gaat via X-road. Deze data-uitwisselingslaag maakt uitwisseling tussen verschillende informatiesystemen mogelijk, zowel in de publieke als private sector. Zo word ook uitwisseling met en tussen alle overheidsdatabases mogelijk. Ieder instantie die gebruikt maakt van meer dan één

database, maakt dan ook gebruik van X-road. Data blijft bij de authoritieve bron; X-road is een infrastructuur, géén centrale database.

Een belangrijk kenmerk van X-road is zijn uniformiteit: er is één API die gebruikt wordt voor alle uitwisselingen. Tegelijkertijd blijft het systeem flexibel, doordat organisaties vrij zijn te kiezen hoe ze hun ICT systemen verder inrichten. Met Xroad kunnen gecertificeerde partijen direct met elkaar communiceren via een beveiligde verbinding; deze is versleuteld en aan beide zijden moeten de partijen zich succesvol authentiseren. Alle communicatie is digitaal ondertekent en time-stamped.

X-road verwezenlijkt het 'only once' principe van e-Estonia: een burger of organisatie hoeft informatie slechts één keer te verstrekken. Door soepele uitwisseling tussen authoritieve bronnen is het niet nodig dezelfde data meermaals te vragen of kopieën van data op te slaan in lokale databases.

Digitale identiteiten

In een digitale samenleving hebben burgers een digitale identiteit nodig. In e-Estonia heeft die digitale identiteit verschillende aspecten. De essentiële bouwsteen van het identiteitssysteem is de Personal Identification Code, een unieke identifier die overal te gebruiken is.

Iedere burger heeft een ID-card, een smartcard die als fysiek en digitaal identiteitsbewijs dient. De chip bevat twee certificaten: een voor digitale persoonlijke identificatie, data signing en encryptie van data, en de ander voor het zetten van een digitale handtekening (die wettelijk equivalent is aan een geschreven handtekening). Deze certificaten zijn onderdeel van een Public-Private Key Infrastructure die beheerd wordt door de overheid. Het digitale supplement op de fysieke ID-Card wordt Digi-ID genoemd. Ook is het mogelijk om een smartphone als identiteitsbewijs te gebruiken met Mobile-ID. En speciale simkaart vervult dan dezelfde rol als de smartcard op de ID-card.

Ervaringen en succesfactoren

Dat het digitale identiteiten- en authenticatiesysteem een succes is, blijkt uit de succesvolle lancering van e-Residency. e-Residency is het digitale inwonerschap van de digitale samenleving. Het is geen volwaardig burgerschap van Estland of een bewijs van inwoning. E-Residency is een transnationale digitale identiteit. Hiermee kan een niet-inwoner toegang krijgen tot de digitale infrastructuur van e-Estonia. Daarnaast kan een e-Resident gebruik maken van de volwassen authenticatie-infrastructuur voor andere doeleinden. E-residency is een stimulans voor ondernemerschap in Estland door niet-inwoners.

Idensys

Idensys is een systeem voor online authenticatie van burgers, zowel bij de overheid als bij private partijen. Het ministerie van Economische zaken opereert als eigenaar van het Idensys afsprakenstelsel. Idensys biedt plaats voor meerdere aanbieders van authenticatiemiddelen; deze kunnen ook door private partijen verstrekt worden. Dit betekent dat een publieke partij gebruik moet kunnen maken van het BSN om een burger te identificeren, ook als deze inlogt met een middel wat verstrekt is door een partij die zelf het BSN niet mag gebruiken. Hiertoe is het BSN-koppelregister opgezet.

Met één Idensysmiddel kan een gebruiker bij verschillende organisaties inloggen. Maar niet iedere organisatie behoeft hetzelfde betrouwbaarheidsniveau (i.e. Level of Assurance of LoA); daarom zijn de Idensys middelen op verschillende niveaus verkrijgbaar (2 t/m 4). Voor inloggen op niveau 2 is een combinatie van gebruikersnaam en sterk wachtwoord voldoende, op hogere niveaus komt daar een tweede factor bij, zoals een one-time password via sms of het invoeren van een pin in een app. Zo'n tweede factor kan verschillen per aanbieder; ook hier heeft de gebruiker dus de keuze.

Er zijn momenteel vier aanbieders van Idensys middelen, en er kan bij zo'n 25 partijen met Idensys ingelogd worden: o.a. de belastingdienst, verschillende gemeenten, zorgorganisaties en enkele private organisaties.

Wat biedt Idensys?

Idensys biedt één systeem waarmee burgers, met een authenticatiemiddel uitgegeven door een partij naar hun keuze, in principe bij alle dienstaanbieder kunnen inloggen, zowel privaat als publiek. De reikwijdte van Idensys is dus erg groot; zo'n beetje iedere organisatie kan er op aansluiten. Doordat er verschillende middelenaanbieders zijn, is het voor de burger ook nog eens een flexibel systeem; hij kan immers zelf kiezen welk authenticatiemiddel zijn voorkeur heeft en deze bij een verscheidenheid aan organisaties gebruiken.

Wat is de status?

Er zijn momenteel 4 aanbieder van Idensys middelen: KPN, CreAim, Digidentity en SecureIdentity. Daarnaast vervullen KPN, CreAim en Digidentity ook de rol van makelaar en ondersteunen zij dienstverleners in het aansluiten op Idensys.

Private en publieke partijen kunnen zich momenteel aansluiten bij Idensys. Reeds zijn er zo'n 25 partijen aangesloten, zowel publiek (o.a. belastingdienst en gemeenten) als privaat (bijv. een aantal zorgverzekeraars) en enkele zorgorganisaties.

Architectuur

Het Idensys systeem moet een enorme variëteit aan authenticatiemiddelen en dienstaanbieders kunnen omsluiten. Om ervoor te zorgen dat alle gegevensuitwisselingen goed verlopen, maakt Idensys gebruik van de rol van makelaar. De makelaar fungeert als het connectiepunt tussen de dienstaanbieders en de authenticatiediensten. Ook treed de makelaar op als dienstverlener richting de dienstaanbieders, met diensten rondom de implementatie en het beheer van Idensys.

Idensys valt onder het Afsprakenstel Elektronische Toegangsdiensten, wat tevens het afsprakenstelsel is voor eHerkenning (het authenticatiemiddel voor bedrijven richting overheid). Hierin zijn alle afspraken opgenomen die nodig zijn om Idensys te laten werken.

Een voorbeeld daarvan zijn de afspraken over de betrouwbaarheidsniveaus (LoA). Ieder niveau biedt de dienstaanbieder een bepaald niveau van betrouwbaarheid van de authenticatie. Daarbij horen eisen aan het authenticatiemiddel en het identificatieproces bij uitgifte van het middel. Zo kunnen dienstaanbieders er op vertrouwen dat het authenticatiemiddel betrouwbaar genoeg is voor de dienst die zij aanbieden.

iDIN

iDIN is een authenticatiesysteem ontwikkeld door Nederlandse banken. Klanten van banken kunnen ermee inloggen bij overheidsinstanties en private partijen. Daarvoor gebruiken ze dezelfde inlogmiddelen die zij ook voor online bankieren gebruiken. iDIN lijkt qua gebruikersinteractie op het veel gebruikte iDEAL; maar in plaats van na het inloggen een financiële transactie te doen, vind er een transactie plaats van attributen die de dienstaanbieder vraagt.

Het afsprakenstelsel rondom iDIN wordt beheerd door de Betaalvereniging Nederland. Zeven verschillende banken fungeren momenteel als zogenoemde 'issuer' van het inlogmiddel. Momenteel is het mogelijk om bij zo'n tien verschillende organisaties in te loggen met iDIN; o.a. de belastingdienst, maar ook private partijen zoals verzekeraars.

Zowel iDIN als Idensys kunnen dus bij overheidsinstellingen gebruikt worden voor authenticatie. Daarnaast bestaat ook DigiD nog steeds; deze kan alléén bij publieke organisaties gebruikt worden, niet bij private. De onderstaande plaat geeft een overzicht van deze verschillende authenticatiemiddelen.

Wat biedt iDIN?

iDIN is een authenticatiesysteem wat optimaal gebruik maakt van het feit dat een bank zijn klanten op hoog betrouwbaarheidsniveau identificeert en authentiseert. Hier werd de facto al gebruik van gemaakt in identificatie processen door de zogenoemde '1 cent transactie' waarmee de te identificeren persoon bewijst eigenaar te zijn van een bepaald rekeningnummer, en daarbij ook de tenaamstelling van die rekening wordt vastgesteld. Zulke 1 cent transacties worden door derde partijen gebruikt, die daarmee dus meeliften op de veilige authenticatie van banken.

Met iDIN wordt deze veilige authenticatie benut door banken zelf, door een authenticatiemiddel aan te bieden aan hun klanten, waarmee zij bij derde partijen kunnen inloggen. De klant hoeft hier niets nieuws voor aan te vragen; hij heeft zich immers al geïdentificeerd bij de bank. Ook is de klant al in het bezit van een veilige manier van inloggen; deze wordt immers gebuikt voor internetbankieren.

iDIN biedt dus groot gemak aan de gebruikers; ze gebruiken een middel wat ze reeds hebben om te authentiseren op een manier die hen ook al bekend is van internetbankieren en iDEAL. Ook voor andere partijen, zoals dienstverleners die iDIN als inlogmiddel accepteren, is iDIN gemakkelijk. Er wordt immers gebruik gemaakt van een volwassen ecosysteem.

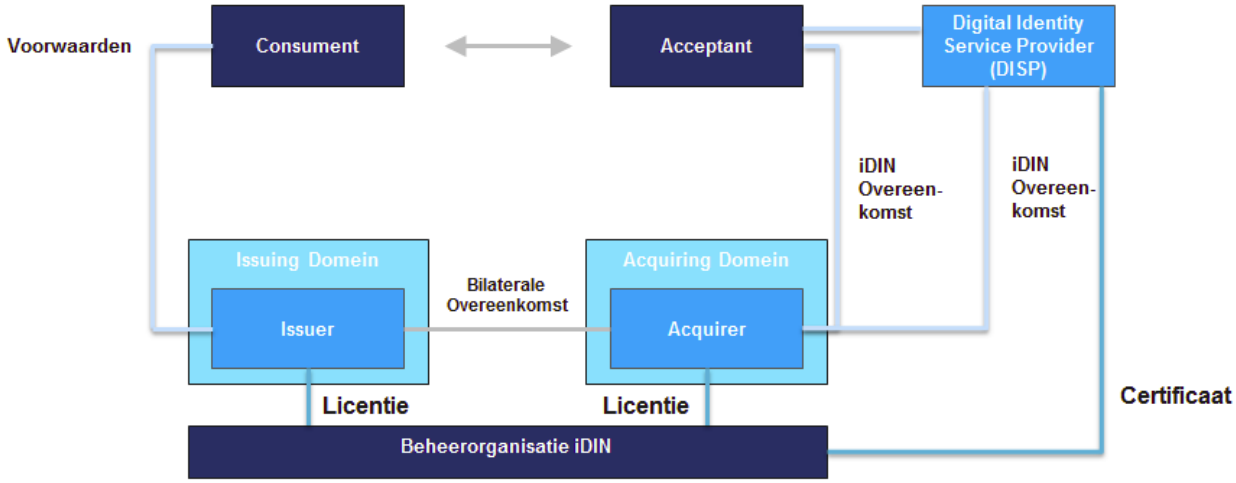
Wat is de status?

iDIN is momenteel volledig operationeel. Er zijn op dit moment 11 acceptanten, waaronder de belastingdienst, enkele verzekeraars, en verschillende bedrijven in de financiële sector.

Er zijn vier aquirers: ABN AMRO, ING, Rabobank en de Volksbank. Momenteel zijn er twee partijen die de rol van DISP vervullen; CM Payments en Signicat. De huidige issuers zijn ABN AMRO, ING, Rabobank, Triodos Bank en de Volksbank.

Architectuur en beveiliging

De issuer is de uitgever van het authenticatiemiddel; bij iDIN zijn dit altijd (consumenten)banken. Aan de ontvangende kant zijn drie verschillende rollen. De acceptant is de dienstverlener waarbij de consument zich authentiseert; deze accepteert de inlog met iDIN, vandaar de naam. Zo'n acceptant kan dat natuurlijk alleen doen, als deze is aangesloten op het iDIN systeem. Dat kan op twee manieren. Het eerste is door een overeenkomst te sluiten direct met een (ondernemers)bank, de aquirer in bovenstaand schema. De tweede manier is via een Digital Identity Service Provider, die de implementatie en beheer van iDIN als dienst aanbiedt aan acceptanten.



Afbeelding 13: Rollen binnen iDIN, bron: https://www.idin.nl/identiteitdienstverleners/

IRMA

I Reveal My Attributes (IRMA) is een oplossing die is gericht op het delen van attributen; oftewel, eigenschappen van een persoon zoals de naam, het geslacht, of het feit dat de persoon ouder dan 18 jaar is. Alleen de attributen die nodig zijn voor een transactie worden gedeeld, zonder andere informatie te verstrekken. Het IRMA systeem werkte initieel met een 'smart card', maar de ontwikkelingen zijn verschoven naar een smartphone applicatie. Dit betekent dan ook dat IRMA focust op het verstrekken van attributen in een digitale wereld, en niet, zoals met de smartcard mogelijk was, bij de slijter op de hoek. Attributen kunnen wel opgehaald worden in de fysieke wereld door een combinatie van dataoverdracht via van QR codes en face to face authenticatie.

Op dit moment is IRMA nog in ontwikkeling. Er zijn twee pilots geweest in 2015 met Universiteit Twente en Universiteit Nijmegen, nieuwe pilot zijn in ontwikkeling. IRMA wordt nu beheerd door stichting Privacy By Design. Alle bijbehorende software is open source en gratis.

Wat biedt IRMA?

De belangrijkste waarde die IRMA beoogt te bieden is het privacy vriendelijker maken van online authenticatie. IRMA maakt het mogelijk per attribuut te bepalen of deze verstrekt wordt; zo kun je al je andere attributen, die niet van belang zijn voor de transactie, privé houden. Vergelijk het met het kopen van alcohol in de supermarkt; je kan als klant alleen je gehele identiteitsbewijs laten zien, om aan te tonen dat je ouder bent dan 18. IRMA biedt de mogelijk alleen het attribuut 'ik ben ouder dan 18' te delen met bijvoorbeeld een webshop voor alcoholische dranken.

Hiervoor worden twee middelen aangeboden aan de gebruiker zelf: de IRMA app en de MijnIRMA website. In de IRMA app zijn de verschillende attributen zijn opgeslagen. Wanneer je wilt inloggen bij een bepaalde website, die daarvoor attributen vraagt, kun je deze via de app verstrekken. Als aanvulling op de app is er de mijnIRMA website, waarop het gebruik van de IRMA gevolgd kan worden. Hier staan bijvoorbeeld log gegevens van welke attributen op welk moment aan welke partij zijn verstrekt. Dit is dan wel in de vorm van meta data; de inhoud van de attributen zelf blijft onbekend voor de stichting achter IMRA, om zo te voldoen aan het privacy by design principe. Ook kun je op de website je IRMA blokkeren indien je telefoon gestolen is.

Om IRMA te laten werken is er een ecosysteem van verschillende partijen nodig. IRMA faciliteert uitgifte van attributen door geverifieerde partijen. Bijvoorbeeld SURFnet geeft attributen uit, waarmee iemand kan aantonen een student of medewerker te zijn van een bepaalde onderwijsinstelling. Uitgifte gebeurt zowel digitaal als fysiek, door het scannen van een QR code met de app.

Ook biedt de stichting de benodigdheden aan relying parties (zij noemen ze "controleurs") voor het implementeren van IRMA op hun website, waarmee ze van hun gebruikers attributen kunnen ontvangen. De relying parties zullen dit momenteel vooral zelf moeten doen, maar het zou goed in het ecosysteem passen als dit door commerciële partijen als dienst aangeboden gaat worden; vergelijkbaar met payment service providers die o.a. iDEAL transacties verzorgen voor webshops.

Wat is de status?

Momenteel zijn er vier manieren waarop attributen verstrekt worden. Via SURFconext, de authenticatiedienst van SURFnet, kunnen attributen worden opgehaald zoals de onderwijsinstelling en status van student of medewerkers. Momenteel kan dit alleen nog voor de Radboud universiteit. De tweede manier is via iDIN; daarmee kunnen attributen zoals naam en adres worden opgehaald bij de eigen bank van de gebruiker, maar geen financiële attributen zoals rekeningnummer. Met deze attributen uit iDIN kunnen, via de stichting, attributen uit het BIG register gehaald worden. De vierde manier is door zelf attributen direct in de app te laden, door middel van het uitlezen van de gegevens op de chip van een identiteitsbewijs.

Daarnaast geeft de stichting aan pilots voor te bereiden met de Radboud universiteit, SURFnet en Alliander, maar hier is geen verder informatie over beschikbaar.

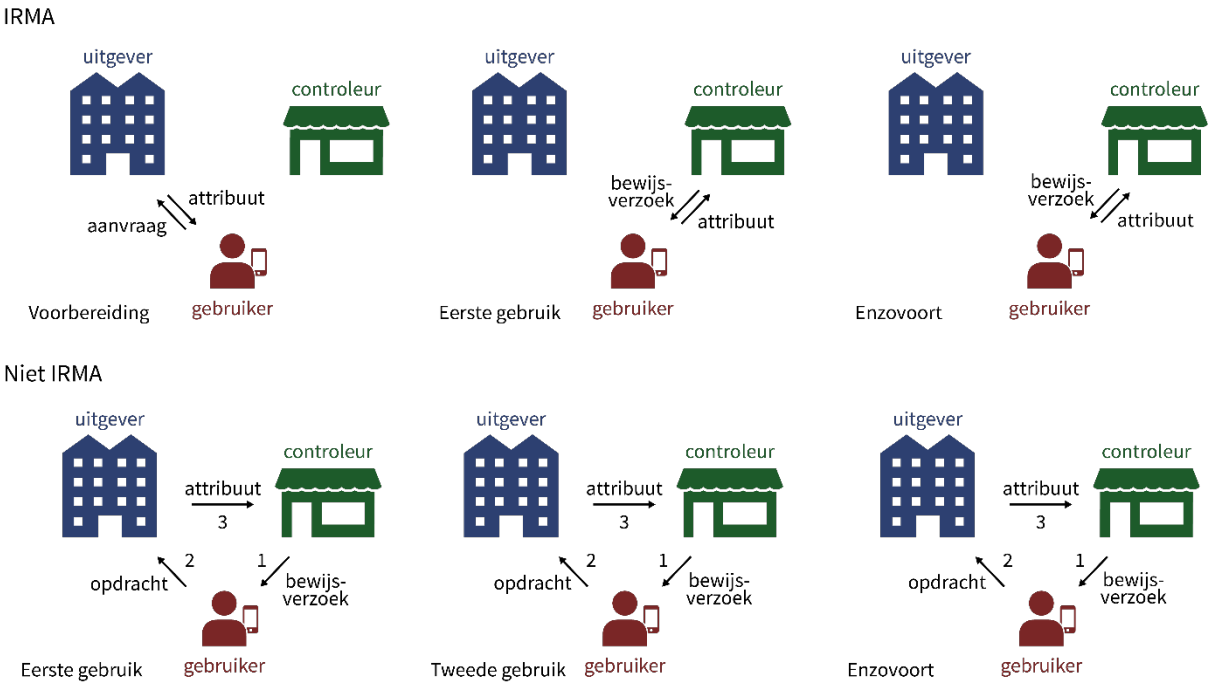
Identity management

Interessant is dat IRMA géén betrouwbaarheidsniveaus (Levels of Assurance) hanteert. Het LoA systeem stelt bepaalde eisen aan de vaststelling van identiteit ten behoeve van de uitgifte van een authenticatiemiddel. Deze eisen zouden dan moeten worden opgenomen in het IRMA afsprakenstelsel. Dit zou betekenen dat er toezicht op moet worden gehouden door de stichting, maar ook dat de uitgevers van attributen meer/ander werk krijgen om aan deze eisen te voldoen. Door géén gebruik te maken van LoA, worden de relying parties dus zélf verantwoordelijk voor het beoordelen van de betrouwbaarheid van attributen. Idealiter worden zij juist ontzorgd van deze taak door een afsprakensysteem als IRMA.

Architectuur

IRMA onderscheid zich van andere systemen door een decentrale architectuur. Hiermee wordt bedoeld dat er geen centrale opslag is van de attributen bij de een “identity broker”, een partij die identiteitsgegevens beheert en kan verstrekken aan relying parties. Wel staan de attributen (ook) opgeslagen bij de partij die ze heeft uitgegeven, maar deze kan daarna niet meer zien waar de attributen verstrekt worden. En natuurlijk staan alle attributen van een gebruiker in de IRMA app. Alle controle ligt daarmee bij de gebruiker zelf.

In onderstaande figuur wordt het verschil weergegeven tussen de IRMA architectuur, en een architectuur waarbij de attributen steeds door de uitgever aan de relying party verstrekt worden.



Afbeelding 14: Uitgever en controleur komen in het IRMA ecosysteem nooit met elkaar in contact. Bron: Stichting Privacy By Design

Beveiliging

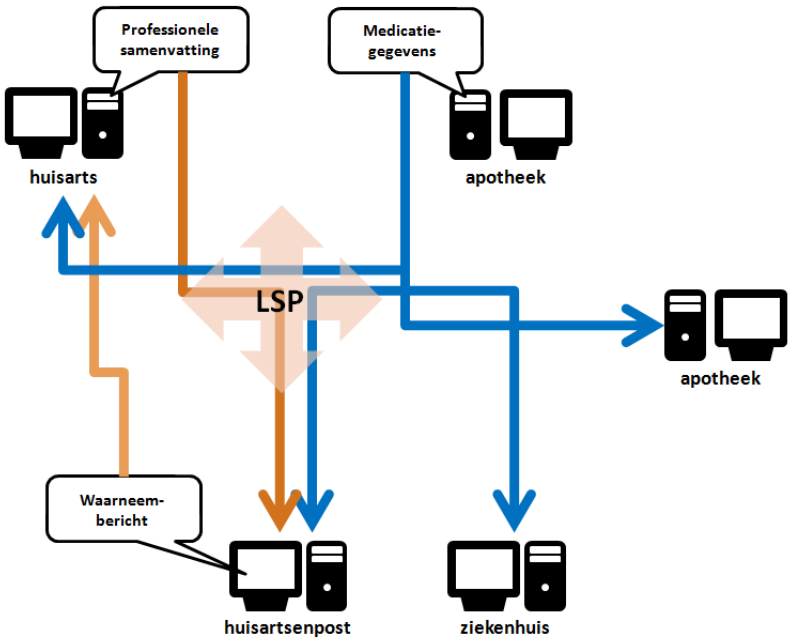
Het IRMA ecosysteem maakt gebruik van een public-private key cryptografie om de attributen mee te beveiligen. Een uitgever van een attribuut zet een digitale handtekening op het attribuut. De controleur (relying party) kan door middel van deze handtekening controleren dat het attribuut daadwerkelijk is uitgeven door de partij die dat claimt (authenticiteit) en dat het attribuut ‘onderweg’ naar de controleur niet gemanipuleerd is (integriteit).

Landelijk Schakelpunt

Het Landelijk Schakelpunt (LSP) is een infrastructuur om medische gegevens inzichtelijk te maken voor verschillende zorgverleners. Wanneer patiënten hiervoor toestemming hebben gegeven, kunnen zorgverleners via het Landelijk Schakelpunt (LSP) medische gegevens bij andere zorgverleners op een veilige en betrouwbare manier inzien, maar uitsluitend wanneer dit voor de behandeling noodzakelijk is.

Wat biedt het Landelijk Schakelpunt?

In het LSP staan het Burger Service Nummer (BSN) en welke aangesloten zorgverleners een bijbehorend medisch dossier beschikbaar hebben. Zo kunnen het (samengevatte) medisch dossier dat wordt bijgehouden door de huisarts, en het medisch dossier bijgehouden door de apotheek (vaak het medicatieoverzicht genoemd) worden ingezien door (waarnemend) huisartsen, apothekers en medisch specialisten.



Afbeelding 15: Inzage in medische gegevens via het LSP. Bron: VZVZ

Het medisch dossier blijft de verantwoordelijkheid van de zorgverlener en staat niet in het LSP. Het LSP is géén centrale database; ieder medisch dossier blijft opgeslagen bij de verschillende zorgverleners. In die zin is het dus verwarrend om te spreken over hét medisch dossier van een patiënt; technisch gezien is dit een verzameling van medische dossiers.

De patiënt geeft echter wel één keer toestemming tot inzage van deze dossiers via het LSP. Hierbij kan hij apart toestemming geven aan de huisarts en aan de apotheek om het betreffende dossier beschikbaar te stellen voor inzage. De patiënt kan ervoor kiezen een gedeelte van zijn dossier af te schermen, waardoor dit niet ingezien kan worden door andere zorgverleners.

Het LSP heeft een mijn-omgeving waarop burgers kunnen inloggen met DigiD om een inzage-overzicht te bekijken van welke zorgverleners welke medische gegevens hebben opgevraagd. Ook biedt de mijn-omgeving gebruikers de mogelijkheid om zich te abonneren op een melding bij inzage van gegevens. Zorgverleners kunnen alleen een vereiste selectie van persoonlijke en medische gegevens inzien. Bovendien kan men in overleg met zorgverleners vragen bepaalde gegevens af te schermen.

Wat is de status?

Momenteel zijn alleen huisartsenpraktijken (89%), apothekers (94%), huisartsenposten (96%) en ziekenhuizen (81%) aangesloten op het LSP.

Voor patiënten zelf is het mogelijk om de logging-gegevens over inzages door zorgverleners te zien op de mijn-omgeving, maar zij kunnen zelf nog niet hun medische gegevens inzien via het LSP.

Architectuur en beveiliging

Medische data behoeft goede veiligheid. Onderdeel daarvan is de authenticatie van degenen die toegang krijgen tot gegevens. Zorgverleners authentiseren zich met een smartcard: de zogeheten UZI-pas, wat staat voor Unieke Zorgverlener Identificatie. Deze worden uitgegeven door de overheid. Ook vind er uitgebreide logging plaats in het LSP: wie er wanneer welke gegevens heeft ingezien. De patiënt over wie de gegevens gaan kan deze logging ook bekijken.

Het is een misverstand dat het landelijk schakelpunt een centrale database is waar alle medische gegevens in staan opgeslagen. Het LSP is een verwijsindex, de medische dossiers blijven opgeslagen bij de authoritieve bronnen, de zorgverleners zelf. Dit is een veiligere architectuur dan wanneer alles op één plek staat; desondanks moeten alle afzonderlijke medische dossiers nog steeds goed beveiligd zijn.

Ervaringen en succesfactoren

In wezen fungeert het LSP als een PDS voor het inzien en delen van medische gegevens, maar is hierin beperkt. Zo kunnen gebruikers in het LSP nog niet de eigen medische dossiers inzien. Door verschillende partijen wordt gesproken over een koppeling tussen het Landelijk Schakelpunt en Persoonlijke Gezondsheidsdossiers. Een koppeling met het PGD zou het mogelijk maken om via het LSP de eigen medische informatie in te zien, op te slaan en te kopiëren. Vooralsnog is die communicatie eenzijdig; de patiënt kan de gegevens downloaden in zijn persoonlijke gezondheidsdossier, maar nog niet vanuit die PGD toestemmingen beheren of verzoeken doen tot het aanpassen van de data bij de authoritieve bron.

Het LSP blijft echter omstreden, vooral om redenen van veiligheid en privacy. Recentelijk presenteerde de Huisartsenkring Amsterdam in samenwerking met de Universiteit van Amsterdam een decentraal alternatief systeem voor het centrale LSP dat een deel van deze zorgen zou kunnen wegnemen.

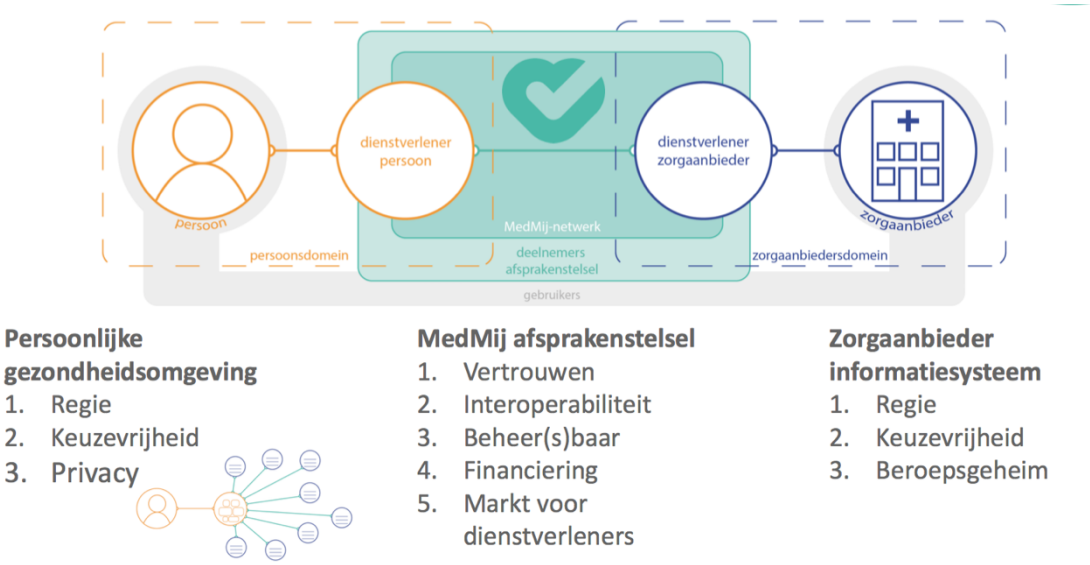
MedMij

Tijdens de MedMij conferentie gaven van 18 mei gaven de verschillende MedMij projectleiders een overzicht van MedMij. In presentaties over de architectuur, juridische kant en standaarden achter MedMij, werd duidelijker hoe het de afgelopen jaren is ontwikkeld en wat de huidige status is.

Wat biedt MedMij?

In eerste instantie is het afsprakenstelsel MedMij erop gericht om patiënten een veiliger gevoel te geven en uiteindelijk betere hulp te kunnen verlenen. Voor patiënten is het namelijk lastig om alle informatie bij elkaar te houden. Er moeten vaak dezelfde informatie verstrekt worden als een patiënt naar een andere locatie moet; er wordt slecht uitgewisseld tussen verschillende ziekenhuizen.

Er zijn initiatieven voor 'persoonlijke gezondheids omgevingen' maar door gebrek aan standaarden kunnen zij moeilijk opschalen. MedMij zou voor die standaarden voor gegevensuitwisseling moeten zorgen; het biedt een afsprakenstelsel om vertrouwen te waarborgen. Daarin staan o.a. beveiligingsafspraken, aansluitvoorwaarden en technische standaarden.

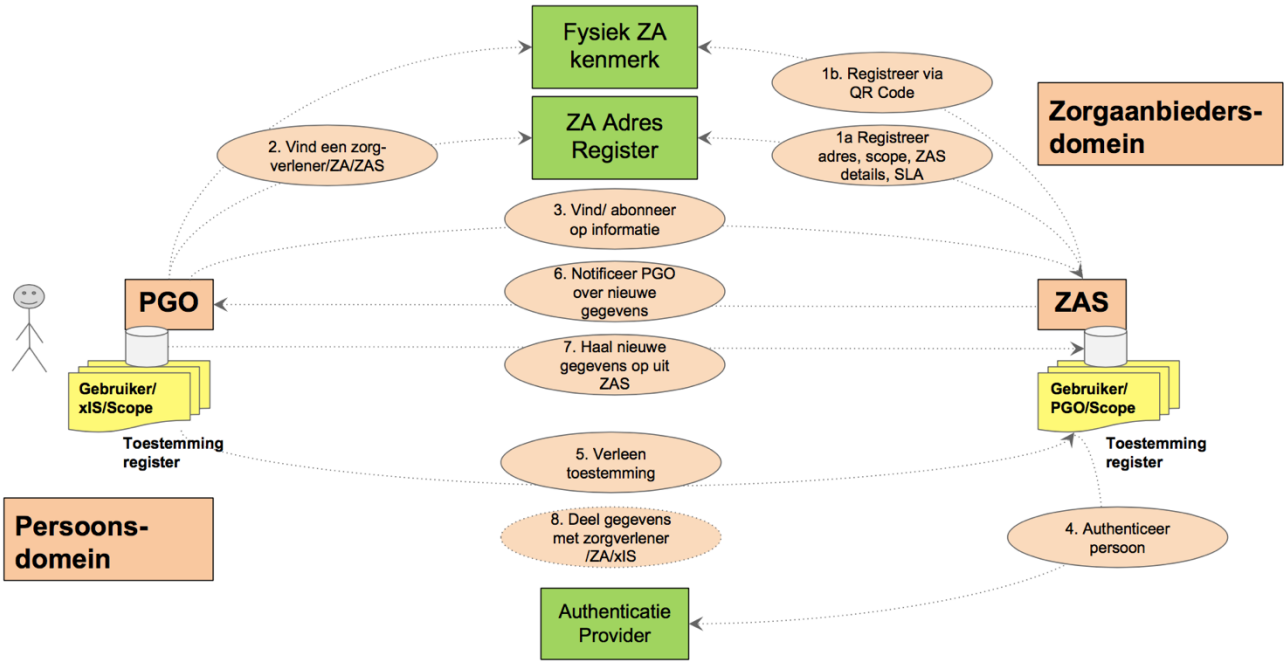


Afbeelding 16: Afsprakenstelsel MedMij

MedMij kan zorgen voor regels rond de uitwisseling van persoonlijke data. De voorwaarden daarvoor moeten worden vastgelegd. Zo is er bijvoorbeeld een bewerkersovereenkomst nodig vanuit zorgaanbieders met dienstverleners. De zorgverlener bepaald daarnaast nog steeds wat relevant is om op te nemen in het medisch dossier. 'Goed hulpverlenerschap' is hierop van toepassing.

Gegevens en infrastructuur

Tijdens de conferentie werd duidelijk dat MedMij geen infrastructuur gaat bouwen. Gegevens zullen bewaard worden in een PGO omgeving, of in de systemen van de arts. Om zorgverleners, personen en data aanbieders te identificeren is eIDAS substantieel of hoog nodig. Dit is vereist om met zorggegevens te werken en delen. Deelnemers aan het stelsel moeten elk jaar aantonen dat ze voldoen aan de normen. Er wordt daarmee ook niks aan data vastgehouden in de uitwisseling. MedMij zal afspraken vastleggen waarover een persoon voorkeuren over kan uitspreken, zoals het aan/uitzetten van uitwisseling tussen partijen. De stappen die gezet worden bij het uitwisselen van gegevens is te zien in de onderstaande functionele architectuur van MedMij.



Afbeelding 17: Functionele architectuur van MedMij

Standaarden

De gegevensuitwisseling die in een stelsel als MedMij moet gaan plaatsvinden is zeer complex. Niet alleen moeten zorgverleners onderling gegevens kunnen uitwisselen, ondanks dat zij verschillende systemen gebruiken, ook moet de zorgverlener met de patiënt kunnen uitwisselen, die weer een andere applicatie gebruikt. Om dit mogelijk te maken zijn standaarden nodig. Niet alleen moeten zulke standaarden vastleggen op welke manier gegevens uitgewisseld worden, ook de gegevens zelf moeten aan standaarden voldoen (inclusief metadatering). Bijvoorbeeld, wanneer een patiënt een bepaald medicijn gebruikt, moet dat in alle systemen met dezelfde naam worden aangeduid (e.g. wetenschappelijke naam vs merknaam) en de dosering moet in alle systemen op dezelfde manier worden aangeduid (e.g. overal “50 mg” en niet ook “0,05 g”).

Standaardisatie is niet nieuw in de medische sector. Er zijn al veel standaarden, die goed werken. Daarom gaat MedMij geen nieuwe standaarden ontwikkelen. Zij sluiten zich aan bij bestaande standaarden, en maken deze zo nodig specifieker voor het MedMij stelsel. Deze standaarden worden ook opgenomen in het afsprakenstelsel.

Rol voor de overheid

De overheid zou een rol kunnen spelen in de ontwikkeling van MedMij d.m.v. financiering van partijen die willen deelnemen in het stelsel. Mogelijk als eenmalige financiering om het aanbod van gegevens op gang te brengen, of structureel om leveranciers van gegevens een perspectief te bieden.

Daarnaast ziet MedMij zichzelf als aanvulling op wet en regelgeving, wat erop duidt dat er vanuit de overheid een wettelijk kader verwacht wordt rond PDM. Hoe dit precies ingevuld zou kunnen worden is onzeker, en zal mogelijk pas duidelijk worden bij doorontwikkeling van het stelsel.

Waar loopt MedMij tegenaan

Een lastig punt voor het stelsel, is dat sommige mensen vertegenwoordiger zijn voor een ander. Deze vertegenwoordigers moeten bij medische gegevens kunnen wanneer dat nodig is.

Daarnaast zijn is de kwaliteit van gegevens uit wearables nog niet altijd helder of bekend. In hoeverre kan er uitgegaan worden van de correctheid van de metingen?

Huidige status van MedMij

Er lopen momenteel drie pilots rondom het MedMij stelsel; deze worden “kickstarts” genoemd. In een pilot worden informatiestandaarden en (delen van) het afsprakenstelsel van MedMij is de praktijk getoetst.

De eerste pilot wordt gedaan door het Havenziekenhuis in Rotterdam en Curavista. Samen met COPD patiënten testen zij gegevensuitwisseling rondom de ziektelastmeter voor COPD. Hierin houdt een patiënt zelf bij hoe hij zijn klachten ervaart, en enkele waarden die daar een invloed op hebben (o.a. beweging, vermoeidheid, emoties). In dit overzicht ontbrak altijd de waarde ‘longinhoud’ omdat deze in het ziekenhuis gemeten moet worden. Deze waarde wordt in deze pilot nu wél uitgewisseld, volgens het MedMij afsprakenstelsel.

Het Radboud UMC en IQhealthcare werken samen aan een tweede pilot, waarin patiënten via het Landelijk Schakelpunt inzage krijgen in de professionele samenvatting van hun medisch dossier. Deze pilot is momenteel aan het opstarten, de eerste resultaten worden in voorjaar 2018 verwacht.

In een derde pilot wordt het Persoonlijke Gezondheidsdossier van leverancier Zorgbelang verder ontwikkeld om volgens het MedMij stelsel gegevens te kunnen uitwisselen tussen patiënten en zorgverleners. Hierbij is een belangrijke rol weggelegd voor metingen die de patiënt zelf thuis doet, bijvoorbeeld bloedsuiker meten, maar ook de metingen van een Fitbit of smartscale. Een belangrijke ontwerpkeuze in deze PGO is dat de data decentraal opgeslagen blijft, volgens het ‘linked data’ principe. Fitbit data bijvoorbeeld wordt wel opgehaald in de PGO, maar niet gekopieerd; zo blijven de servers van Fitbit de authoritieve bron en is de data in de PGO altijd up to date.

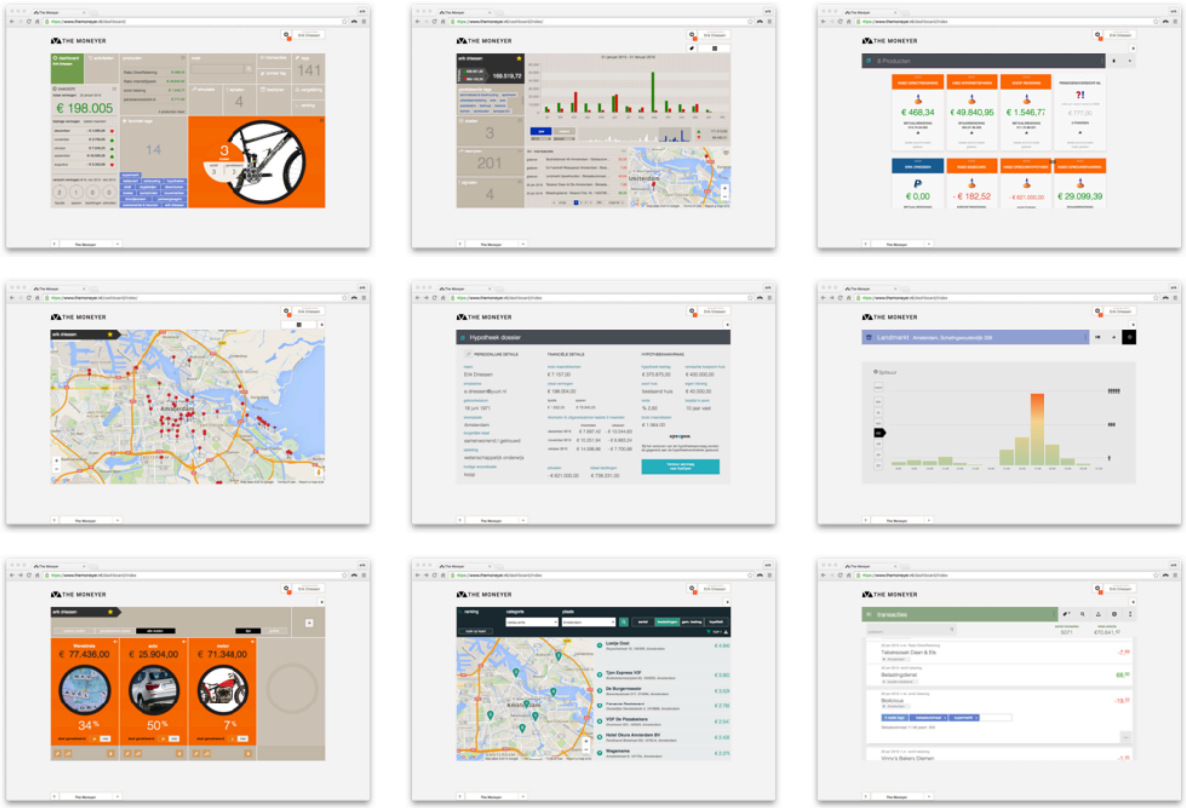
The Moneyer

The Moneyer is een dienst voor personal finance management, een specifieke insteek van PDM. Je kunt met The Moneyer je transactieinformatie van verschillende bankrekeningen aggregeren en analyseren. Het bestaat sinds 2012 en is beschikbaar voor consumenten en wordt door banken gebruikt, ook (juist) in het buitenland. Met de komst van PSD2 krijgt personal finance management een steviger fundament met meer mogelijkheden.

Wat biedt The Moneyer?

The Moneyer is een dienst rond financiële data van een individu, personal finance management; Nederlandse organisatie, gevestigd in Amsterdam. The Moneyer is opgericht in 2011 en is op dit moment voor consumenten bruikbaar. De kern van Moneyer is het bij elkaar brengen van de financiële gegevens van diverse bankrekeningen. Dit wordt vervolgens versleuteld en geanonimiseerd opgeslagen op een beveiligde Zwitserse server. Hier kan The Moneyer vervolgens analyses op doen en kijken naar zaken als bestedingspatronen. Het is o.a. mogelijk om financiële doelen te stellen en een persoonlijke financieel plan te koppelen aan de data. De gebruiker kan daarnaast zelf bepalen of hij/zij dit wil delen met andere service aanbieders.

Naast transactiedata is ook pensioendata in het geheel betrokken.



Afbeelding 18: Voorbeelden gebruik The Moneyer (bron: The Moneyer).

Het consumentenproduct wordt gebruikt om nieuwe features die ontwikkeld zijn te testen. Uitontwikkelde producten worden daarna ook aan banken aangeboden. The Moneyer werkt op dit moment met de meeste Nederlandse banken samen aan Proofs-of-Concept voor een nieuw mobiel product.

Doorontwikkeling

Op dit moment werken ze aan The Moneyer Cards (TMC), hetgeen met een real-time koppeling met banken werkt. Start in Duitsland omdat daar deze koppelingen nu al mogelijk zijn, nog voor de introductie van PSD2. Daarnaast wordt ook in Engeland gewerkt aan een introductie. TMC werkt met machine learning voor analyses. Daarbij wordt uitgegaan van een product gebaseerd datamodel om de informatie uit de transacties te

analyseren. Machine learning maakt het mogelijk nieuwe producten snel te duiden en afwijkende transacties op te sporen voor de gebruiker. Daarmee is TMC, met focus op financiële data, een ver ontwikkeld PDM-initiatief.

Uiteindelijk zal de financiële sector om platformen gaan draaien, meer dan om eindproducten. The Moneyer wil een van die platformen zijn.

Ervaringen en succesfactoren

In eerste instantie werkte The Moneyer met een hiërarchisch informatiemodel dat de wereld van de consument en haar transacties centraal stelde. Dat bleek moeilijk op te schalen. Nu wordt er een datamodel gebruikt vanuit merchant perspectief dat beter werkt, ook voor machine learning.

Voor The Moneyer is het consumentenproduct een belangrijk middel voor testen. De uitontwikkelde producten worden daarna door banken ingezet. Dit gemengde business model is een belangrijke succesfactor.

In Duitsland is wetgeving in de stijl van PSD2 al veel eerder ingevoerd. Dat heeft geleid tot het Financial Transaction Services protocol (FinTS) waarmee online bankieren wordt ondersteund, voortbouwend op eerdere protocollen als het Homebanking Computer Interface uit 1996.

Verwachtingen richting de overheid

Aandachtspunt vanuit The Moneyer is de verzwakking die de PSD2 regulering heeft gekregen in de Regulatory Technical Standard (RTS). De RTS beschrijft niet meer *wat* de bank ter beschikking moet stellen. Daarmee is de basis voor sterkere marktwerking verzwakt. Uiteindelijk zal de financiële industrie een platformindustrie worden. Inmiddels lopen er al gesprekken over een PSD3 die de tekortkomingen moet opheffen. De overheid zou daarbij sterker moeten optreden in de regulering, zowel om behoorlijk wetgeving te realiseren maar ook toe te zien op implementaties. “Cowboys” kunnen rond PDM er voor zorgen dat de reputatie van de sector en van nieuwe initiatieven snel te gronde gaat, zeker in een branche waar de vertrouwenspositie zwak is.

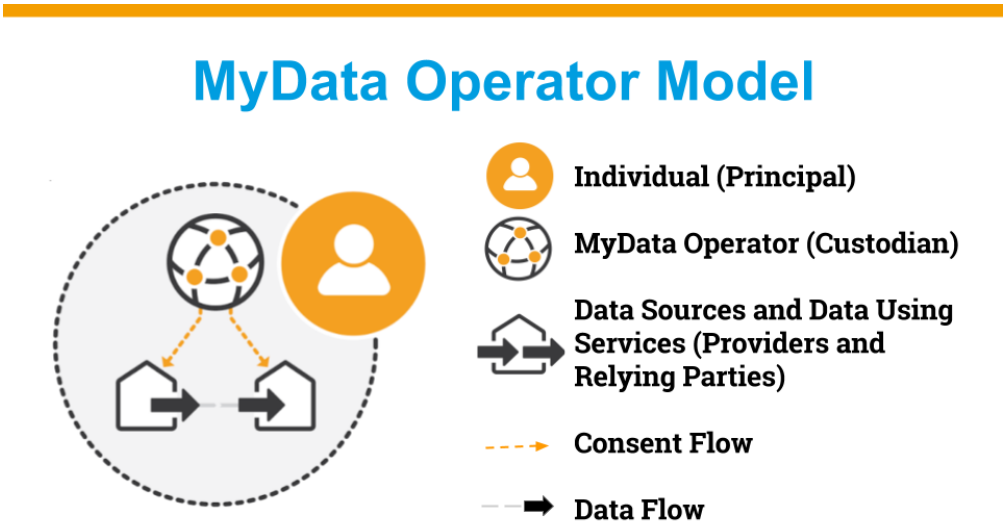
MyData

MyData is een Fins kennisplatform rond PDM waar onderzoekers en organisaties bij aangesloten zijn. Het is in de eerste plaats een behoeftesteller. Door MyData wordt in 2017 voor de tweede keer een PDM conferentie georganiseerd. Daarnaast zijn er meerdere werkgroepen rond MyData en de ambitie bestaat om een open infrastructuur neer te zetten voor personal data services. Deze moet generiek worden over sectoren en internationaal bruikbaar zijn en via API's te benaderen. De MyData infrastructuur bevat zelf geen data, maar organisaties kunnen erop aansluiten. Personen krijgen daarbinnen de mogelijkheid om consent te geven of en welke data uitgewisseld mag worden.

Wat biedt MyData?

MyData biedt in de eerste plaats een sterke en veelzijdig uitgewerkte visie op persoonlijke data. De kern van MyData is het idee dat individuen de controle zouden moeten hebben over hun eigen persoonlijke data. Dit betekent dat individuen het recht én de praktische middelen hebben om hun data te beheren, dat data een herbruikbare grondstof is die technisch gezien makkelijk bruikbaar en deelbaar is, en dat er een open ecosysteem is rond data.

Om deze visie te kunnen bewerkstelligen werkt MyData aan diverse ontwikkelingen. Het MyData Operator Model is een uitwerking van de principes, rollen en processen die nodig zijn voor PDM volgens de MyData visie. Hierin zijn bijvoorbeeld verschillende modellen voor het geven van consent uitgewerkt.



Figuur 1: de MyData operator stelt de individu in staat zijn data te managen door middel van een account.

MyData beschouwt de MyData Operator als een facilitator van accounts, die ieder individu kan gebruiken. Met zo'n operator account kun je verschillende datastromen beheren. Een account wordt gehost door de Operator, net zoals een email account wordt gehost door bijvoorbeeld Gmail/Google. Inherent aan MyData is het idee dat er meerdere operators zijn, die mogelijk ook verschillende functionaliteiten aanbieden. Vergelijk het bijvoorbeeld met Gmail/Google versus Outlook/Microsoft; van beide is de essentie het versturen van mail, maar hoe deze functies worden aangeboden, welke nevenfunctionaliteiten er zijn, en hoe de accounts integreren met andere functionaliteiten verschilt. Dit zal ook gelden voor de MyData operators; belangrijk is dat ondanks verschillende functionaliteiten, de accounts wel interoperabel zijn. Net zoals je met ieder emailadres naar ieder ander emailadres kan mailen.

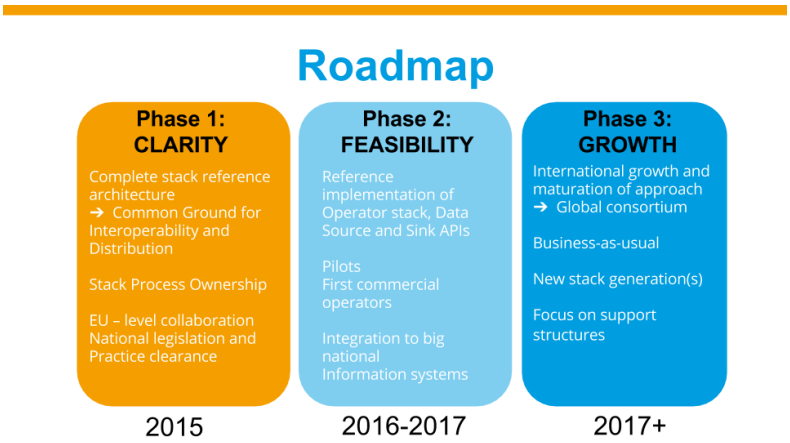
Wat is de status?

Een recente ontwikkeling binnen de MyData alliance is het uitwerken van business modellen voor verschillende sectoren. Momenteel wordt gewerkt aan het verder technische ontwikkeling, toewerkend naar pilots. Hierbij is het de bedoeling dat pilots in verschillende sectoren plaatsvinden, en focussen op verschillende (technische)

aspecten van MyData, zodat deze van elkaar kunnen leren. Een aantal van die aspecten zijn consent management via UMA, opslag van persoonlijke data, anonimisatie en aggregatie van data en de het genereren van persoonlijke gezondheidsdata door middel van self tracking.

Ook worden de MyData Operators nu opgezet. Als nieuwe rol in het al tijden draaiende data-ecosysteem is dit geen sinecure. Maar uiteindelijk zal het MyData systeem niet kunnen werken zonder de Operators; zij vormen de link tussen de individuen en de partijen die hun data verwerken. Ook data-aanbieder en dienstaanbieders zullen uiteindelijk hun systemen moet aanpassen om te voldoen aan het MyData model.

Daarnaast organiseert MyData nu voor de tweede maal de MyData conferentie. Op dit evenement komen zo'n 1000 deelnemers samen om kennis te delen over personal data management in t algemeen, en specifiek de manier waarop MyData dat voor ogen heeft.



Figuur 2: Ontwikkelingsroadmap van MyData.

UMA

Consent management in MyData is gebouwd op UMA, oftewel User Managed Access. UMA is een toepassing van OAuth2.0. UMA stelt resource owner (in dit geval, de individu over wie de persoonlijke data gaan) in controle over de authorisaties die nodig zijn voor het delen van data.

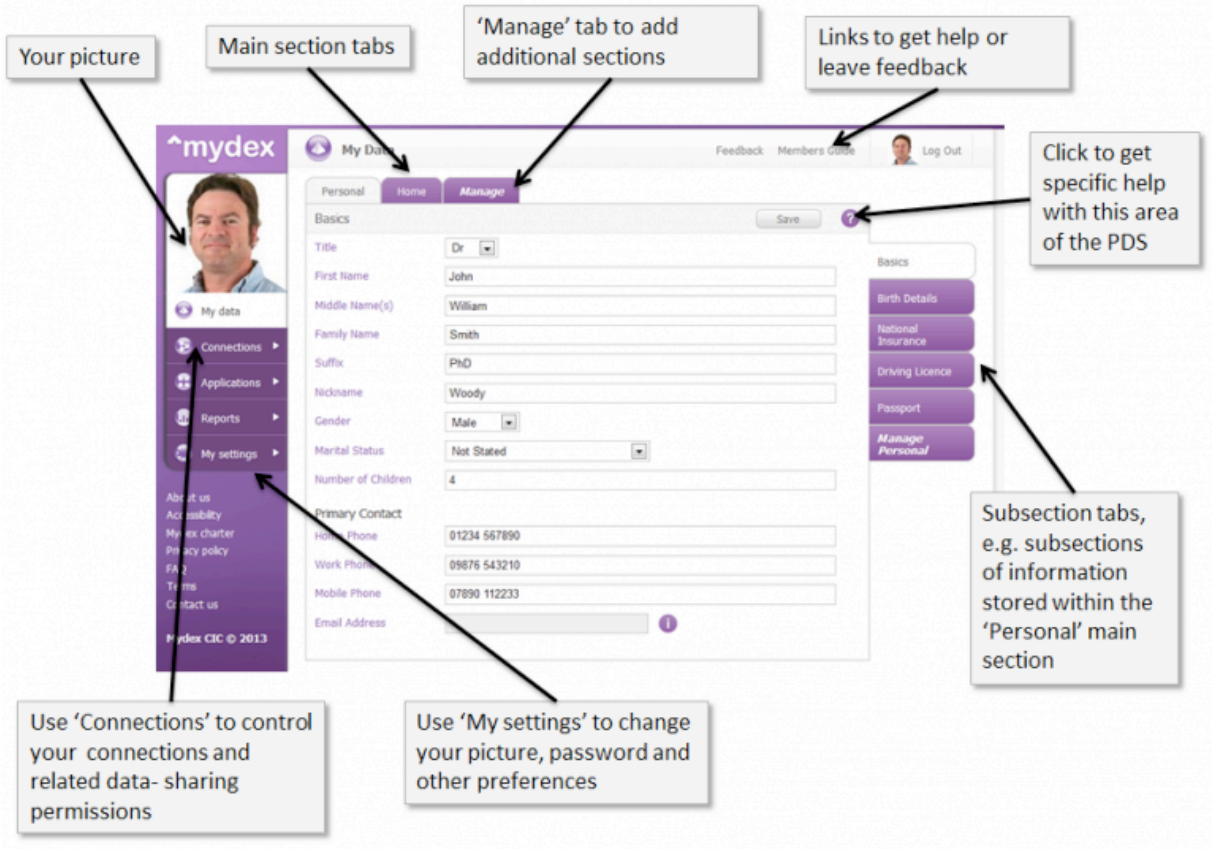
Mydex

Mydex is een personal data service en trust framework dat erop gericht is om data veilig te bewaren en delen. Mydex is opgericht in 2007, door een aantal investeerders. Het is neergezet als stichting (not for profit bedrijf CIC in UK), om te voorkomen dat winst een te grote rol zou spelen. Mydex is op het moment bruikbaar voor consumenten, er kunnen contactgegevens uitgewisseld worden. Het platform is nog in ontwikkeling: de ambitie is om andere attribute providers te koppelen aan het systeem. Dit initiatief is vooral gericht op de markt in Groot-Britannië, maar is open voor hergebruik elders.

Mydex is een interessant internationaal initiatief omdat er een uitgebreide omgeving gebouwd is waaraan externe partijen gekoppeld kunnen worden en zich sterk open opstelt. De specificaties voor aansluiting zijn bijvoorbeeld vrij gepubliceerd en kunnen als voorbeeld dienen voor andere initiatieven.

Wat biedt Mydex?

Mydex levert een personal data (management) service (personal data store genoemd door hen) gebaseerd op een publiek beschikbaar trust scheme. Dit trust scheme is gebaseerd op uitgangspunten, vergelijkbaar met die van Qiy.



Afbeelding 19: Elementen in de Mydex PDS (bron:pds.mydex.org).

Zeven basisdiensten maken deel uit van Mydex:

- Cluster Collaboration Platform
- GDPR Compliance Package
- Consent Management
- Identity as a Service
- Secure Digital Letterbox
- Secure Attribute Exchange Platform
- Personal Data Stores

Dit gaat verder dan een pure PDS, maar omvat ook zaken als een berichtenbox, community management etc. Deze worden aangeboden voor bedrijven, burgers en overheden. Voor de UK overheid maken ze deel uit van de Digital Marketplace van gov.uk, een specifieke omgeving voor diensten te gebruiken door de overheid (in de G-Cloud, met specifieke overheidstarieven).

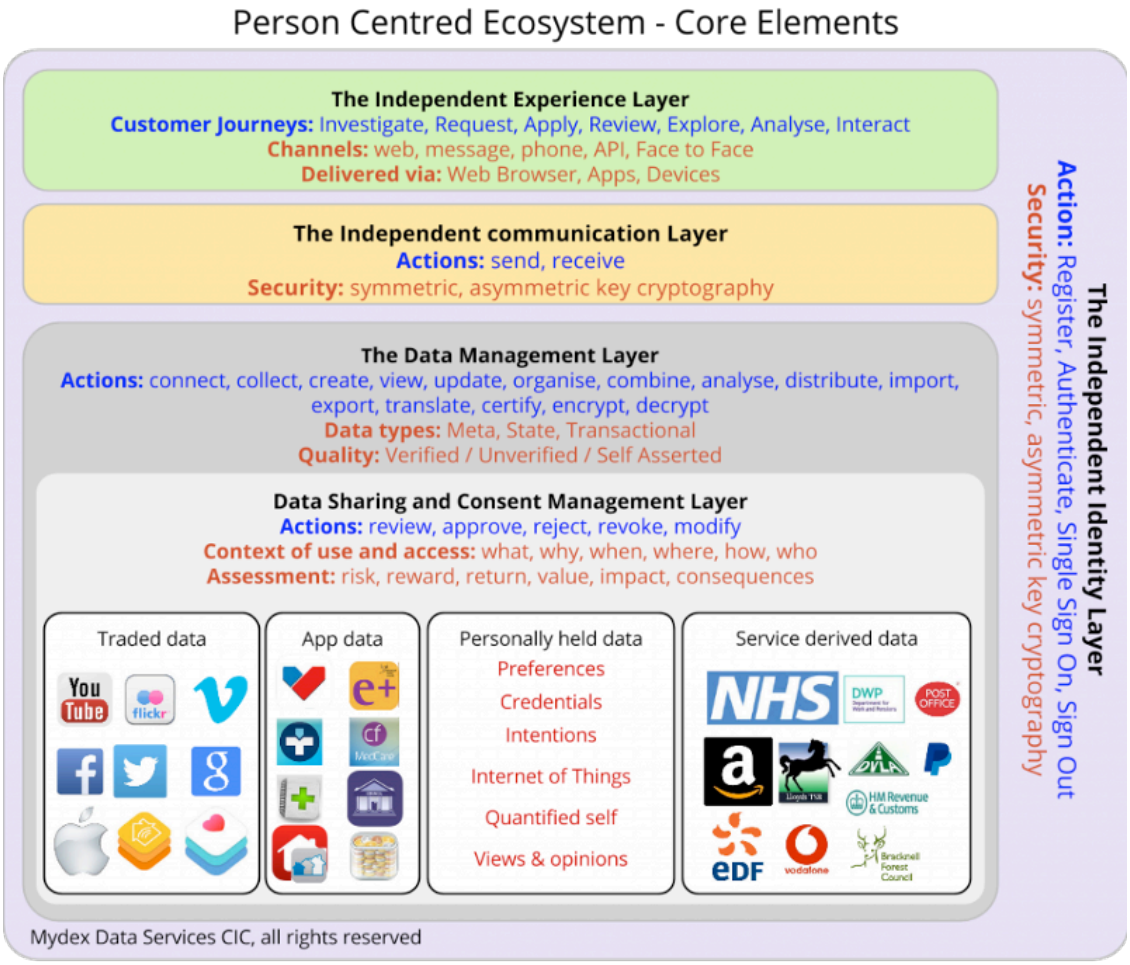
Wat is de status?

Mydex bestaat nu tien jaar, maar is nog niet opgeschaald. Het platform is al zes jaar live, meer dan 30 organisaties zijn aangesloten en er zijn duizenden gebruikers. In Schotland is men bezig met de ondersteuning van een gemeente met een combinatie van PDS elementen, in Wales en Engeland wordt een verbinding gelegd tussen NHS en het sociale domein. Mydex is ISO27001 gecertificeerd, een belangrijke veiligheidsstandaard.

Architectuur

Voor het PDS deel van Mydex werkt het met centrale opslag van data in de cloud en beveiligde uitwisseling van attributen en data. Daarnaast gaat Mydex uit van een onafhankelijke gebruikerservaring (experience layer). Het wil met name interoperabiliteit bevorderen tussen technische standaarden.

Mydex heeft ook een identity service, maar niet gekoppeld aan een formele identiteit, wel met breder identity management. In Groot Brittannië wordt niet gewerkt met een centrale identiteit zoals het BSN.



Afbeelding 20: verschillende lagen vormen samen de Mydex PDM

Doorontwikkeling

Mydex ontwikkelt verder via domeinspecifieke initiatieven. Daarnaast staat het open voor hergebruik van het framework en mogelijk een deel van de componenten. Daarnaast is men actief in Europees onderzoek voor doorontwikkeling.

Ervaringen en succesfactoren

Volwassen persoonlijk data management is een generatiewisseling. Nu al speelt PDM, maar het is niet transparant. GDPR en PDS2 kunnen daarin een enorme versnelling brengen: transparantie en portabiliteit. In de private sector heeft Mydex in de afgelopen karen sterke weerstand tegen PDM ondervonden. Bedrijven zijn primair gericht op lock-in, waarbij de data wordt afgeschermd. Bedrijfsleven en overheid hebben een paternalistische houding ten opzichte van de consument of burger.

Belangrijk is PDM niet groots en meeslepend te brengen: wanneer het verhaal groot wordt gemaakt (wat het in principe is) wordt het door zo velen omarmd dat er uiteindelijk niets meer gebeurt. Werk vanuit kleine, gerichte toepassingen binnen een regio of een domein, waar direct zichtbare toegevoegde waarde ontstaat.

Wat verwacht men van de overheid?

De overheid moet de randvoorwaarden helder neerzetten voor PDM. Het moet vertrouwen faciliteren, zodat burgers of consumenten kunnen zien dat een dienstverlener zich aan bepaalde regelgeving houdt. Op dit manier worden PDM dienstverleners beoordeeld en gecontroleerd.

Only Once

Only Once is opgericht in 2013, nadat het bedrijf €900.000,- aan crowdfunding had opgehaald. De Only Once service moet het makkelijker te maken om attributen zoals contactinformatie uit te wisselen en up to date te houden. De service is bereikbaar via een applicatie op smartphones. Via een persoonlijk adresboek wordt informatie over contacten verzameld. Gebruikers kunnen daarin zelf bepalen welke informatie ze delen, en welke informatie publiek opgevraagd mag worden. De contactinformatie kan via 'kaartjes' gedeeld worden. Only Once is op dit moment bruikbaar en richt zich met name op personen en organisaties die met regelmaat zakelijke gegevens uitwisselen.

Wat biedt het?

- bewaren van gegevens in personal data store
    - Online en cloudbased
    - Organiseer je eigen gegevens op een centrale plek
    - Centrale opslag
    - Zelf data toevoegen
    - Drie verschillende vormen: persoonlijke gegevens, werknemersgegevens, bedrijfsgegevens

- Persoonlijk adresboek:
    - Makkelijk gegevens uitwisselen dmv qr codes
    - Update je eigen contactgegevens, en deze worden ook bij jouw contactpersonen geupdate

- Delen van gegevens
    - E-business cards: openbaar delen van gegevens
    - Overzicht van wat is gedeeld met wie
    - toegang tot gegevens kan were worden ingetrokken.

Wat is de status?

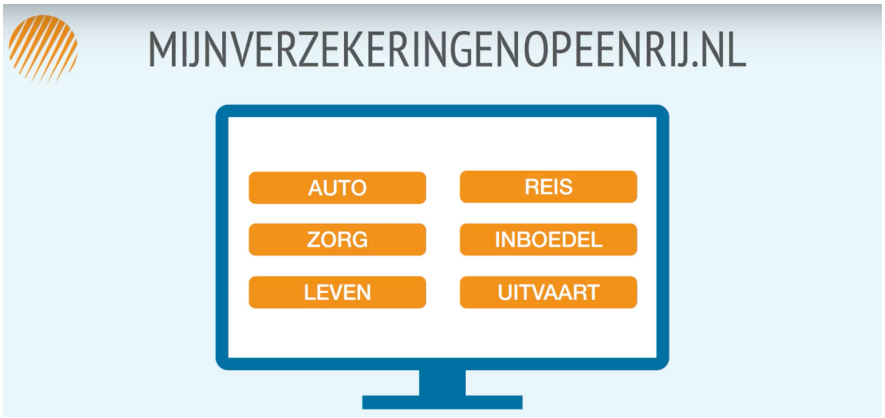
Only Once is volledig operationeel; gegevens over adoptie zijn niet bekend.

Poliskluis

Mijnverzekeringenopeenrij is een initiatief van het Verbond van Verzekeraars. Het is een omgeving waarin de consument alle verzekeringen van alle verzekeraars en gevolmachtigden toe kan voegen. Eén centrale plek zodat verzekeringen niet kwijtraken en altijd een actueel overzicht wordt getoond doordat de polissen max. 1 maand oud zijn. Ook is het mogelijk om gegevens te delen. Dit kan door het machtigen middels een code. Wanneer de gemachtigde de code invoert, krijgt hij/zij inzage in de data waarvoor toestemming is verleend.

Zowel door de consument als door de gemachtigde kan de machtiging op elk moment ongedaan gemaakt worden. Persoonlijk gegevens kunnen uitsluitend worden gedeeld (met de verzekeraars en gevolmachtigden) na toestemming en op initiatief van de consument. Daarnaast kan de consument een pdf maken van alle gegevens en bestaat de mogelijkheid om deze rechtstreeks te delen (via e-mail).

Mijnverzekeringenopeenrij heeft geen database waarin alle gegevens zijn opgeslagen, maar haalt de data op bij de verzekeraar. Alleen polisnummers worden opgeslagen. Bij het uitloggen wordt alle data die is opgehaald bij de verzekeraar weer weggegooid.



Hoe is de ontwikkeling van mijnverzekeringenopeenrij.nl begonnen?

Het initiatief is begonnen naar aanleiding van een onderzoek van de consumentbond, waarin de consument aangaf al de verzekeringen op één centrale plek te willen zien. Het initiatief is in 2013 gestart. In 2014 is er goedkeuring gegeven door het bestuur en in 2015 is de bouw van het platform begonnen. 2016 was het platform zover ontwikkeld dat de eerste verzekeraars aangesloten konden worden.

Nog niet alle verzekeraars zijn ingeschreven. Op dit moment zijn 60 commerciële verzekeringslabels/-merken ingeschreven. Dit komt neer op meer dan 80% van het totaal in Nederland. De verwachting is dat het aantal wordt verdubbeld. Daarnaast worden 60 tot 150 gevolmachtigden verwacht aan te sluiten.

Welke uitdagingen waren er bij de ontwikkeling van mijnverzekeringenopeenrij.nl?

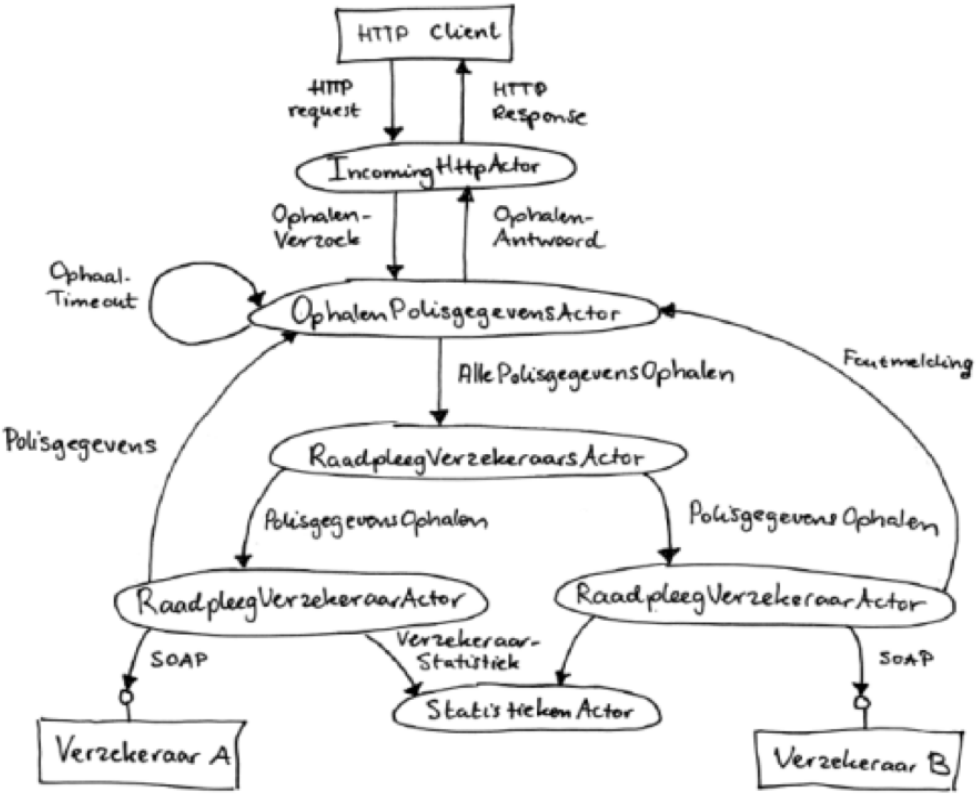
De grootste uitdaging was de authenticatie. Er is geen beschikking over het BSN van de consument om de verzekeringen te kunnen koppelen. Voorheen werden koppelcodes bedacht. Inmiddels gaat er gebruik worden gemaakt van iDIN en iDEAL. In de toekomst wordt ook verwacht hier Idensys aan toe te voegen.

Deze uitdaging is een breder vraagstuk binnen het delen van gegevens. Een van de oplossingen die in het buitenland wordt gebruikt is het ‘privaat BSN’. Dit blijkt daar een werkbare en veilige ontwikkeling.

In hoeverre hebben jullie gewerkt met pilots tijdens ontwikkeling?

Er lopen op dit moment geen pilots. Er zijn en worden wel tests uitgevoerd. In 2015, tijdens het ontwikkelen van het platform is samen met de verzekeraars getest of alle functionaliteiten werken om als verzekeraar aan

te sluiten bij het platform. Daarnaast worden o.a. performance en hack-tests uitgevoerd.



Afbeelding 21: architectuur poliskluis

Maakt mijnverzekeringenopeenrij.nl gebruik van specifieke standaarden?

iDIN en iDEAL standaarden worden gebruikt. Omdat de leveranciers hier nog niet klaar voor zijn, wordt Idensys nog niet gebruikt. De verwachting is wel dat dit in de toekomst ook gebruikt gaat worden. Daarnaast wordt, na het legitimeren, een mijnverzekeringenopeenrij-account aangemaakt. Gebruik van iDIN en iDEAL is alleen voor identificatie.

Welke leerpunten waren er tijdens de ontwikkeling?

Tijdens het ontwikkelen van het platform zijn een aantal lessen geleerd. Ten eerste het feit dat je je moet beperken wat betreft de technische mogelijkheden en functionaliteiten. Wanneer geprobeerd wordt alle mogelijkheden te implementeren, ben je op een gegeven moment het spoor bijster en wordt het onnodig complex. Eenvoud is cruciaal.

Een ander leerpunt heeft te maken met snelheid en ontwikkelingen in de markt. Houdt de laatste ontwikkelingen nauwlettend in de gaten en neem dit mee in het ontwerp. Als de ontwikkeling van een initiatief te lang duurt, wordt je ingehaald door nieuwe ontwikkelingen. Zo moest het platform omgebouwd worden met de komst van iDIN.

Wanneer gaan het live?

Op 1 oktober gaat het platform live met enkele verzekeraars. Verwachting is dat begin 2018 een landelijke uitrol plaats zal vinden. Dit wordt gedaan met een mediacampagne. De verwachtingen zijn dat uiteindelijk minimaal 70% van de Nederlandse bevolking gebruik gaat maken van het platform.

Qiy Afsprakenstelsel

Het afsprakenstelsel Qiy biedt individuen de mogelijkheid persoonsgebonden gegevens uit te wisselen met het publieke en private domein. Gegevensuitwisseling vindt plaats onder regie van de burger, de burger is de centrale spil. Daartoe bevat de persoonlijke Qiy Node, van waaruit gegevens worden uitgewisseld, verwijzingen naar persoonlijke gegevens. De Qiy Node bevat zelf praktisch geen gegevens (de Qiy Node is dus geen traditionele kluis). Het uitwisselen van gegevens via de persoonlijke Qiy Node gebeurt doordat de burger via zijn Qiy Node partij A laat antwoorden op een vraag/vragen van partij B. Het antwoord is beschikbaar gedurende een van tevoren bepaalde termijn.

Indien antwoorden (verklaringen) in geaggregeerde vorm beschikbaar zijn, kan de burger besluiten om de hem betreffende persoonsgegevens die partij B wenst te ontvangen van partij A, in geaggregeerde vorm aan partij A ter beschikking te stellen. Dit kan bijvoorbeeld relevant zijn indien partij B er wel belang bij heeft te weten of de betreffende burger ouder is dan 18 jaar, maar niet de exacte geboortedatum van de betreffende burger hoeft te weten. Ander voorbeeld is wanneer partij B er belang bij heeft om te weten of een burger een bepaald minimum- of maximuminkomen heeft, maar niet de precieze hoogte van het inkomen hoeft te weten.

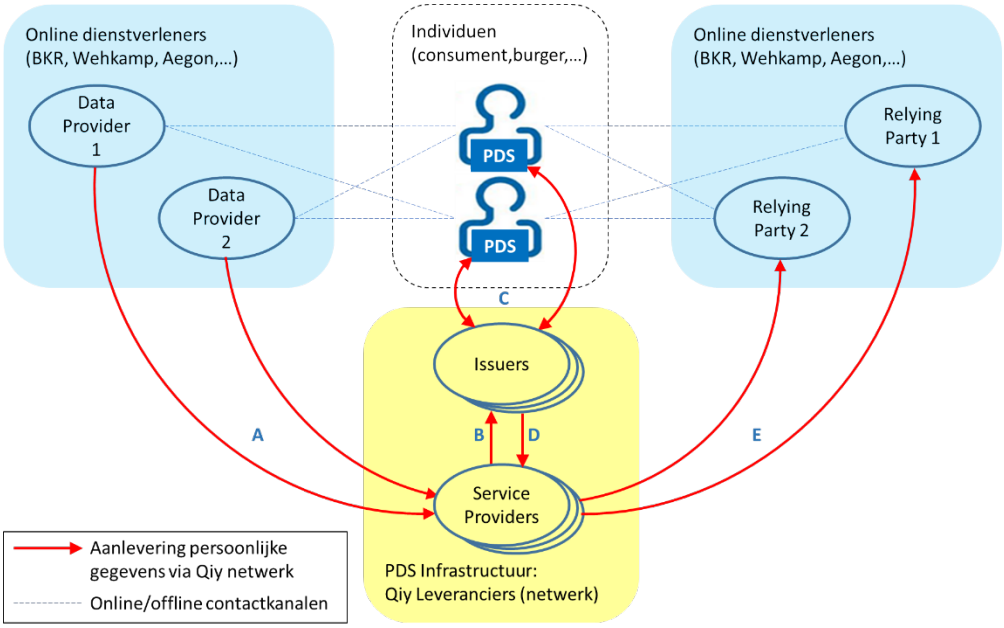
Het afsprakenstelsel Qiy betreft niet de inhoud en semantiek van uitgewisselde gegevens. Qiy maakt het mogelijk ‘gesloten enveloppen’ te routeren. Een partij die bij de routering van dergelijke ‘gesloten enveloppen’ betrokken is kan niet verder kijken dan de eerste eerder en de eerste latere partij in de routeringsketen. Dit betekent dat bestaande informatiemodellen en standaarden kunnen worden gebruikt. Daarnaast maakt Qiy gebruik van diensten voor verificatie van de identiteit en bijbehorende gegevens. Identificatie en authenticatie is geen onderdeel van Qiy zelf.

Qiy Trust Principes

Het afsprakenstelsel Qiy gaat uit van een aantal principes, dat de rechten van het individu omschrijft wanneer deze gegevens uitwisselt via het Qiy Trust Framework. Alle actoren binnen het afsprakenstelsel moeten zich aan deze regels houden.

- *Qiy Node* Een aan mij verstrekte Qiy Node voldoet aan de Qiy Standaard. Via mijn Qiy Node kan ik beschikken over mijn gegevens.
- Mijn gegevens Mijn gegevens mogen alleen met mijn toestemming worden gebruikt. Of die zich nu bevinden bij een organisatie of dat ik ze zelf heb gegeven.
- *Anonimiteit* Ik kan mijn gegevens altijd anoniem delen, behalve als dat wettelijk verboden is. In dat laatste geval kan ik kiezen of ik identificerende gegevens wil verstrekken óf dat ik de transactie af wil breken.
- *Waarborgen* Wanneer een organisatie een waarborg vraagt over mij, moet de gevraagde waarborg echt nodig zijn voor het beoogde doel.
- *Dataminimalisatie* Een organisatie mag mij alleen die gegevens vragen die echt nodig zijn voor het beoogde doel, of die gegevens gevalideerd zijn of niet.
- *Keuze termijn ter beschikking stellen* Ik kan besluiten (een deel van) mijn gegevens éénmalig of voor een bepaalde periode ter beschikking te stellen. Ik kan dit besluit altijd wijzigen, tenzij er een contractuele reden is waarom dit niet kan.
- *Informatieplicht* Als een organisatie mijn gegevens wil gebruiken moeten ze me eerst informeren waarom ze dat willen en hoe vaak.
- *Toegang* Organisaties die deelnemen aan het afsprakenstelsel Qiy zijn verplicht mij ‘toegang’ te geven tot mijn gegevens. Dit geldt niet voor anonieme gegevens, maar verder wel voor alle gegevens die over mij gaan, ook als die ontstaan zijn op basis van gegevens die ik ter beschikking heb gesteld.
- *Delen van mijn gegevens* Organisaties mogen mijn gegevens alleen delen met een andere partij wanneer ik daarvoor toestemming heb gegeven. Deze toestemming kan niet ‘voor altijd’ zijn. De enige uitzondering is dat organisaties dit verplicht zijn vanwege bestaande wet- of regelgeving. Dergelijke uitzonderingen moeten te allen tijde traceerbaar zijn.

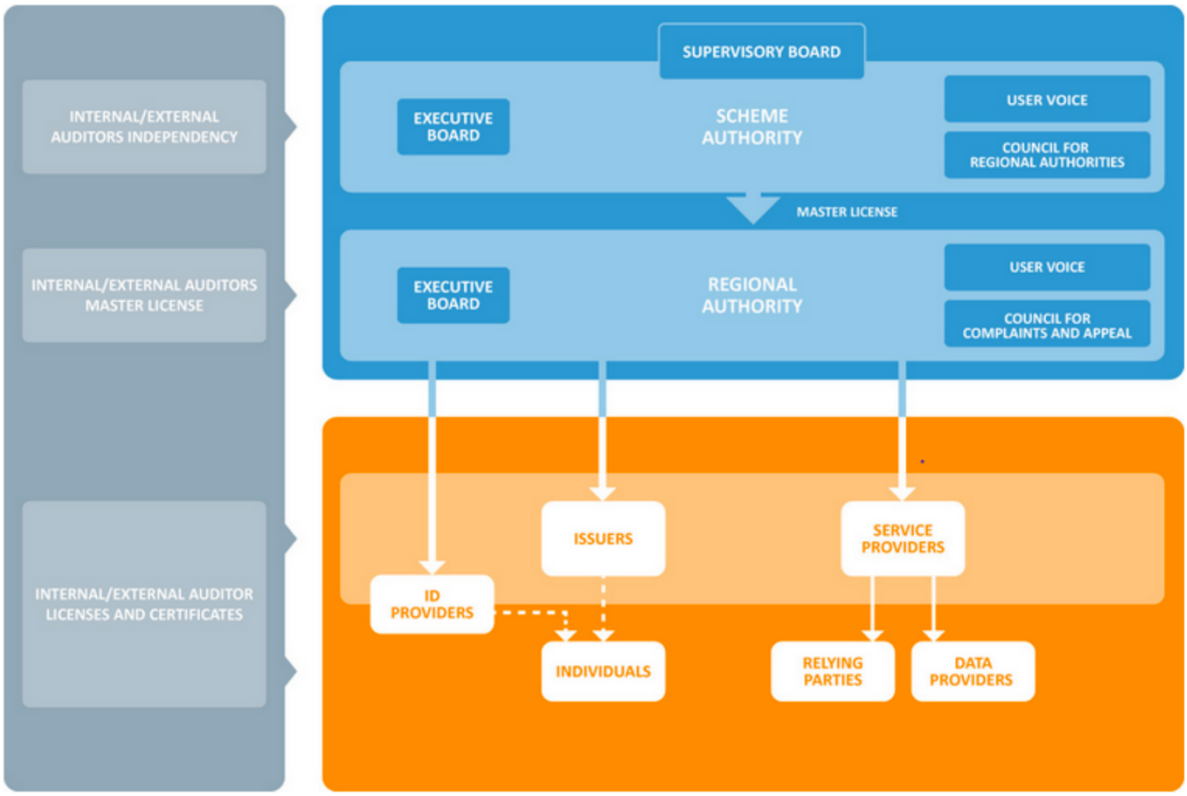
- *Privacy statements* Iedere partij die deelneemt aan het afsprakenstelsel Qiy en mijn gegevens gebruikt of erover beschikt, beveiligt deze gegevens volgens de eisen die daar door Qiy aan gesteld zijn.
- *Bescherming gegevens* Voor iedere organisatie die via Qiy met mijn gegevens te maken heeft, hebben deze Qiy Principes voorrang boven hun eigen privacy statements als de Qiy Principes meer bescherming bieden. Omgekeerd gaan de eigen privacy statements van een organisatie voor als die meer bescherming bieden.
- *Klachten en geschillen*: Als er een klacht is spreek ik eerst de direct betrokken organisatie aan. Dat kan ik doen via hun website. Als dat geen goed resultaat oplevert, mag ik de Geschillencommissie inschakelen.



Afbeelding 22: Uitwisseling van persoonsgegevens via het Qiy Netwerk

Het afsprakenstelsel is in ontwikkeling sinds 2007. Op dit moment lopen er diverse pilots met Qiy, waarvan Gemeente Boxtel de meest concrete is (InnoValor (2016) *Haalbaarheidsstudie Qiy pilots*), naast de inzet van Qiy bij Aegon middels de Dappre app. Deze laatste toepassing werkt al.

Het beheermodel is weergegeven in onderstaande figuur. De verschillende rollen worden hierna toegelicht.



Afbeelding 23: Beheermodel Qiy.

Voor een uitgebreide beschrijving van de rollen zie Qiy Foundation (2015). Op dit moment vallen de Regional Authority en Scheme Authority nog samen en worden ze ingevuld door Marcel van Galen, een van de oprichters. Uiteindelijk wordt een 7-koppige Authority beoogd. Er is één Issuer, het bedrijf Digital Me dat ook de Dappre app heeft gebouwd.

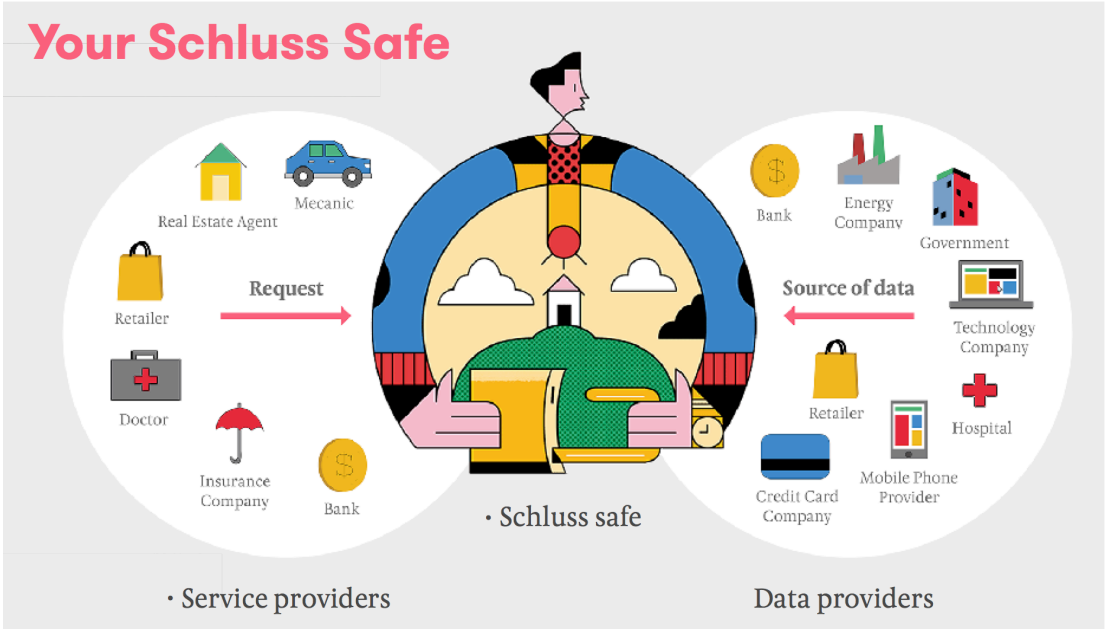
Het stelsel is nog in volop in ontwikkeling, er zijn wel een groot aantal partners betrokken bij het stelsel die in de ontwikkeling ervan investeren. De governance laag is definitief en publiek beschikbaar. De onderliggende schemes en technologie zijn nog niet volledig uitgewerkt en nog in ontwikkeling. Deze zijn ook niet publiek beschikbaar.

Schluss

Schluss is een interessant nieuw initiatief vanuit een maatschappelijk belang van PDM. De coöperatieve structuur met een eenvoudig verdienmodel is daarin een nieuw element ten opzichte van andere ontwikkelingen. Ook het streven naar open source implementaties is vernieuwend. Technisch staat Schluss nog in de kinderschoenen. De komende pilots moeten hier verdere invulling aan geven.

Wat biedt Schluss?

Schluss is een service rond het bewaren van persoonsgegevens, waarbij de gebruiker controle heeft over wat hij deelt, met wie. De toegevoegde waarde van Schluss is dat de gebruiker zelf regie heeft over de data die hij via Schluss uitwisselt, op een veilige manier. De achterliggende visie is dat alleen jij mag bepalen wie wat van je weet en dat de datastroom moet worden omgedraaid. In de kern gaat het om beveiligd attributen uitwisselen. Dat moet zelfs anoniem kunnen, dus met een pseudoniem. Schluss volgt daarmee de benadering van een datakluis.



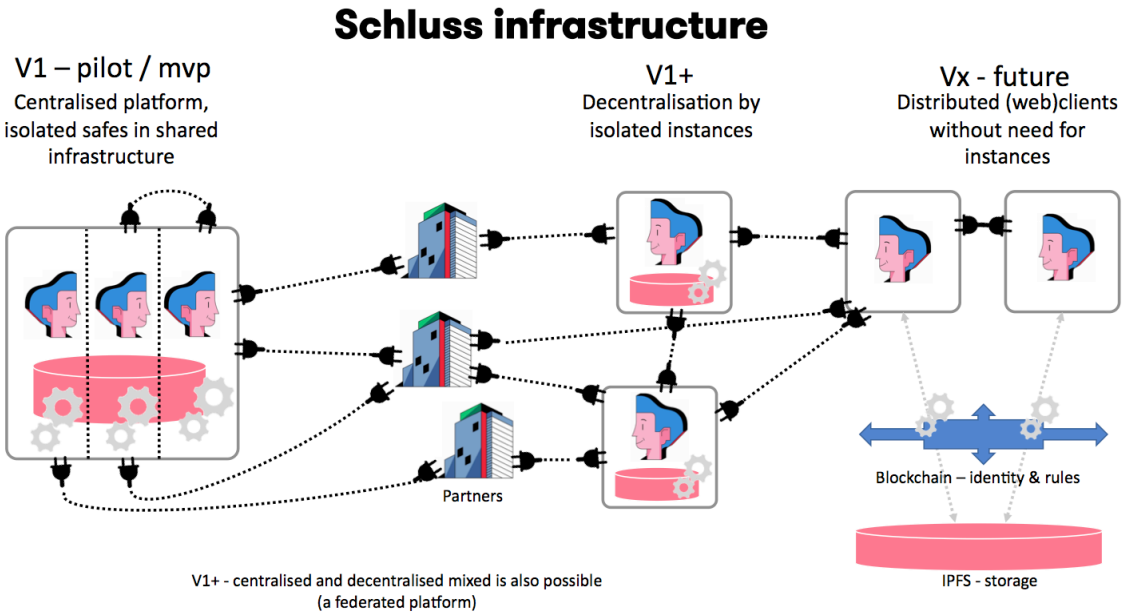
Afbeelding 24: Het Schluss concept.

Wat is de status?

Schluss is opgericht in 2015 en is op dit moment nog in ontwikkeling. De dienst is wel bruikbaar voor consumenten om uit te proberen, het is mogelijk om contactgegevens uit te wisselen en bewaren op Schluss. In 2017 starten er pilots met Schluss bij o.a. Rabobank, KPN en de KvK. De pilots gaan in op verschillende aspecten van het platform, zoals techniek, legal en gebruikerservaring. Op al die vlakken worden minimal viable products gedefinieerd.

Architectuur

Schluss is gestart met een centrale opslag van gegevens. Dit is op termijn niet een wenselijke invulling (Afbeelding 25**Error! Reference source not found.**). Daarvoor wordt nu gekeken naar interplanetary files systems (IPFS), een open source project gestart in 2014. IPFS is een peer-to-peer gedistribueerd filesysteem in de stijl van Bittorrent. Het is nog niet duidelijk hoe IPFS de vereisten van PDM kan realiseren.



Afbeelding 25: Roadmap Schluss

Doorontwikkeling

Als organisatievorm wil Schluss naar een coöperatie, waar de deelnemers leden van de coöperatie zijn, tegen heel lage kosten. Daarmee wil Schluss maximale transparantie realiseren. Juridische uitdaging daarin is hoe je met anonieme leden toch een coöperatie kunt starten. De infrastructuur moet ook open source worden. Om tot die coöperatie te komen is er een tussenfase van ontwikkeling waarin Schluss met een brede maatschappelijke vertegenwoordiging van partijen een stichting wil opzetten. Die gesprekken lopen nu, de stichting is nog niet opgericht.

Ervaringen en succesfactoren

De ervaringen van Schluss zijn nog beperkt. De open source filosofie en het transparantie bedrijfsmodel (betaald, maar betaalbaar) zijn wezenlijk succesfactoren, zo verwacht men.

Wat verwacht men van de overheid

De overheid is meer dan welkom als deelnemer in Schluss om mee te werken aan de ontwikkeling en de stichting.

Social JO!N/HerstelOnline

HerstelOnline is een platform voor een online community van burgers die elkaar ondersteunen bij herstel van indringende levenservaringen. HerstelOnline wordt samen met die burgers ontwikkeld. Er wordt daarbij aangesloten bij de wensen ten aanzien van herstel van de cliëntenbeweging in de GGZ en Verslavingszorg (HEE, LPGGZ en het Zwarte Gat) en er wordt gebruik gemaakt van praktische kennis rondom positieve psychologie (UT Twente). In HerstelOnline staat het meer grip krijgen op je eigen leven en meer meedoen met de samenleving centraal.

In het overheidsbeleid wordt de burger uitgedaagd voorkomende zorg- en welzijn vraagstukken met eigen inzet en van de eigen omgeving op te lossen. Een groot deel van de gebruikers van die voorzieningen beschikt echter over onvoldoende eigen middelen om dat te doen. Zo hebben velen nauwelijks een behulpzaam sociaal netwerk en heeft men weinig vertrouwen in de eigen mogelijkheden.

Wat biedt het?

HerstelOnline wil mogelijkheden bieden voor:

- kennis nemen en delen van herstelervaringen
- uitwisseling van persoonlijke profielen waardoor één op één relaties en groepscontacten online mogelijk worden en offline voortgezet kunnen worden

HerstelOnline onderscheidt zich van gebruikelijke eHealth doordat het geheel vanuit het perspectief van de burger in herstel wordt opgebouwd en diens belangen voorop staan. Het is dus een platform dat past bij de leefwereld van die burgers. Het gaat vaak om hele persoonlijke ervaringen en daarom is vertrouwen een belangrijk onderwerp. Vertrouwen ontstaat door op een volstrekt betrouwbare manier om te gaan met privacy-gevoelige gegevens. Met de toekomstige gebruikers wordt een privacy statuut ontwikkeld. De regels die daarin worden opgenomen dragen eraan bij dat het platform zich onderscheidt van andere social media als Facebook.

Status

Op dit moment is een groep van personen met indringende levenservaringen en ervaringsdeskundigen in Groningen aan het experimenteren met een betaversie van HerstelOnline (HerstelOnline is gebaseerd op een bètaversie van de online community Social JOIN). Het project wordt begeleid door de samenwerkende partijen Social JOIN, Thorax informatieprojecten & advies, iShared en het Centrum voor zelfregie en participatie Groningen.

Doorontwikkeling

Naast doorontwikkeling in andere regio's wil men een tweede spoor volgen: het verzamelen van (niet persoonlijk herleidbare) herstelverhalen. De reden hiervoor is dat er, naast een goed uitgeruste online community, ook voldoende 'voorgeladen' inhoud moet zijn. Met een minimale hoeveelheid inhoud, begrijpen nieuw deelnemende gebruikers eerder wat de bedoeling is en neemt de kans toe dat ze terugkeren. Een online community wordt pas aantrekkelijk bij voldoende inhoud en voldoende deelnemers.

Door meerdere ontwikkelgroepen zal HerstelOnline zich ontwikkelen tot een herstel online functie die aan zeer verschillende groepen in herstel een nuttige ondersteuning kan bieden. Dat is ook nodig, daar de ervaring leert dat een E-community alleen kan functioneren als er veel activiteit op is. Alle betrokken partijen maken deel uit van het netwerk iCW2020, waarin zorg- en welzijnsorganisaties voor formele èn informele zorg, ict-bedrijven, game industrie, bedrijven ontwikkelaars, Universiteit, HBO, eHealth en werkgeversorganisaties zijn verenigd.

Tippiq

Alliander is in de unieke positie dat het een slimme meter in alle huizen heeft zitten. Dat biedt de mogelijkheid een infrastructuur te realiseren die gebruikt kan worden voor persoonsgegevens en het mandaat erover, in relatie tot het huis. Tippiq wil het platform zijn dat de transacties rond toegang tot huizen, apparaten en dingen in het huis op een goede manier kan organiseren, inclusief het privacy vraagstuk. Tippiq is een vertrouwensplatform voor digitale huizen.

Wat biedt het?

Het platform Tippiq biedt de volgende functionaliteit:

- Register van digitale huizen;
- Bewoner kan alles beheren van het huis;
- Data van/naar derden controleren en aan/uit zetten;
- Dienstenbibliotheek;

Validatie van het huis kan nu nog niet. Er zijn proeven gedaan via de IRMA app en iDIN en GBA.

Wat is de status?

Tippiq is drie jaar geleden gestart. Alliander wil als netbeheerder contact hebben met “huizen”. Ze zijn begonnen met onderzoek naar data delen, informatiestromen, en de rol van de gebruiker. Langzamerhand kwamen drie dingen naar boven:

- Register digitale huizen
- Valideren van de huizen (locatie koppelen aan persoon / rollen – eigenaar, bewoner, AirBnb, bewindvoerder, …)
- De toestemming rond het huis zonder de data

Alliander heeft meer dan 120 rollen van mensen i.r.t. het huis geïdentificeerd.

Het platform is beschikbaar. Nu moeten diensten worden ontwikkeld en dat stokt enigszins. Tippiq is in contact met een zorgpartij voor toegang tot het huis en het zorgdossier (vooraankondiging). Het gaat dan nog niet om digitale sloten. Ook werkt een verzekeraar aan verzekeringen rond het gevalideerde en gedocumenteerde huis. Daarnaast wordt er gedacht aan een digitale deurbel: deze gaat over op je mobieltje in plaats van fysiek, ook als je niet thuis bent.

Afbeelding 26: Tippiq brandweer propositie

Doorontwikkeling

Tippiq voorziet de oprichting van een stichting voor beheer en doorontwikkeling van het platform en huisregister, in samenwerking met maatschappelijke organisaties. Daarbij streven ze naar open source. Daaronder kan eventueel een co-operatie van dienstverleners ontstaan, los van de stichting.

Ervaringen en succesfactoren

Het ontwikkelen van een goed lopend platform is niet eenvoudig:

- Overheid wil niet committeren. Financiering ook niet. Ook wordt geen toegang verleend tot basisfunctionaliteit
- Commercieel: eigen belang beschermen. Bedrijven denken “recht te hebben” op de data.
- Kip-ei probleem: platformfinanciering en onderlinge concurrentie op de data.
- Moeten we ook de data regelen? Het kluisje? Conclusie: nee, moet je niet willen!
- Governance: hoe bestuur je dit? Tippiq zelf als validator (via sociale middelen) is ongewenst. Validatie moet je elders doen.
- Gebruikerskant: hoe gaan mensen met data om? Ze zeggen het één (precieze data aan de post geven), maar doen het ander. Gedrag versus intentie.

Wat verwacht men van de overheid

De volgende observaties heeft Tippiq m.b.t. de rol van de overheid:

- Kadaster – kijkt naar Tippiq, maar nog wat vrees.
- Bied experimenteerruimte.
- Uitspraak over de rol die ze kunnen vervullen. De rol van Tippiq kan niet door de overheid worden vervuld, wel experiment en mandaatregeling. Kritisch toekijken, handhaven.
- Niet alleen visierapporten schrijven. Ga wat doen, of zorg dat er wat gebeurt. Stop met “denken voor”, maar faciliteer.
- Toegang tot stelsels of informatie (onder voorwaarden). Voor iedereen, onder gelijke rechten. API tot de overheid. “PSD2 voor de overheid”.

Ydenti

Ydenti is een service die personen helpt om erachter te komen over welkepersoonlijke gegevens organisaties beschikken. Na verificatie van de identiteit van het individu, kan Ydenti helpen bij het uitvoeren van bepaalde rechten. Zoals het recht van inzage, verzet en vergeten. Personen kunnen bijvoorbeeld automatisch inzageverzoeken en vergeetverzoeken aanvragen. Ydenti biedt daarmee een makkelijke manier om van dit soort rechten gebruik te maken. Daarnaast kan de service ook een verhuizing doorgeven, de persoon kiest hierbij met welke organisaties hij deze gegevens deelt. Ydenti kan op dit moment gebruikt worden.

Wat biedt Ydenti?

In de Wet Bescherming Persoonsgegevens, evenals de aankomende Algemene Verordening Gegevensverwerking, zijn verschillende rechten opgenomen die iedere burger heeft ten aanzien van organisaties die zijn of haar persoonlijke gegevens verwerken. Deze rechten zijn o.a.:

- het recht op inzage: een burger heeft recht om te weten welke gegevens een organisatie over hem heeft opgeslagen. Hiertoe kan een verzoek worden ingediend bij de organisatie, waarop zij de gegevens kenbaar moeten maken.
- Recht op rectificatie: het recht om foutieve gegevens te laten corrigeren, danwel ontbrekende gegevens aan te vullen.
- Recht op gegevenswissing (vaak “recht op vergetelheid” of “right to be forgotten” genoemd): de burger heeft recht om de persoonsgegevens die over hem zijn opgeslagen door een organisatie te laten wissen. Hier zitten enkele voorwaarden aan. De gegevens moeten bijvoorbeeld niet langer meer nodig zijn voor het doel waarvoor zij rechtmatig verkregen zijn. Indien de doelmatigheid van de verwerking alleen berust op eerder gegeven toestemming, kan de burger de toestemming intrekken en heeft daarmee recht op gegevenswissing.
- Recht op overdraagbaarheid: het recht de gegevens te kunnen overdragen naar een andere verwerker.
- Recht van verzet bij direct marketing: de burger heeft het recht verzet aan te tekenen tegen het gebruik van zijn persoonsgegevens voor direct marketing doeleinden.

Voor ieder van deze rechten kan de burger een verzoek indienen bij de organisatie die zijn gegevens verwerkt. Niet iedere burger weet dit, of weet hoe ze zo’n verzoek kunnen indienen. Hier helpt Ydenti. Via de services van Ydenti dien je bijvoorbeeld een inzageverzoek in bij jouw internetprovider. De reactie op het verzoek komt terug bij de burger zelf; oftewel, Ydenti kan de persoonsgegevens waar het om gaat niet inzien.

Wat is de status?

De services van Ydenti zijn momenteel beschikbaar. Op dit moment zijn ze kosteloos te proberen. Een Ydentity app is in ontwikkeling.

Data Opslag

Ydenti is een service gerelateerd aan persoonlijke data, maar je kunt er niet je eigen data mee beheren, zoals bij andere PDS. De data blijven namelijk bij de verwerkende organisatie; bij een inzageverzoek krijgt de burger slechts een kopie van de data. Ook wanneer het gaat om wijziging of verwijdering heeft de burger daar geen directe controle over; de verwerker van de gegevens moet dit doen.

Ervaringen en succesfactoren

Data blijft dus opgeslagen bij de authoritieve bronnen; de verwerkers zelf. In die zin is Ydenti minder revolutionair dan Personal Data Services die de burger zélf de authoritieve bron van de gegevens maken. Daarentegen sluit Ydenti naadloos aan op het huidige ecosysteem van dataverwerking en de wetgeving daaromtrent. Ydenti kan dus nu direct zijn waarde bewijzen; er hoeft niet eerst een ecosysteem omheen te groeien met een kritieke gebruikersmassa, zoals bij sommige andere PDS wel het geval is.