Autoriseren op maat in drie dimensies

De Polis Papers (3): Draaien met die kubus!

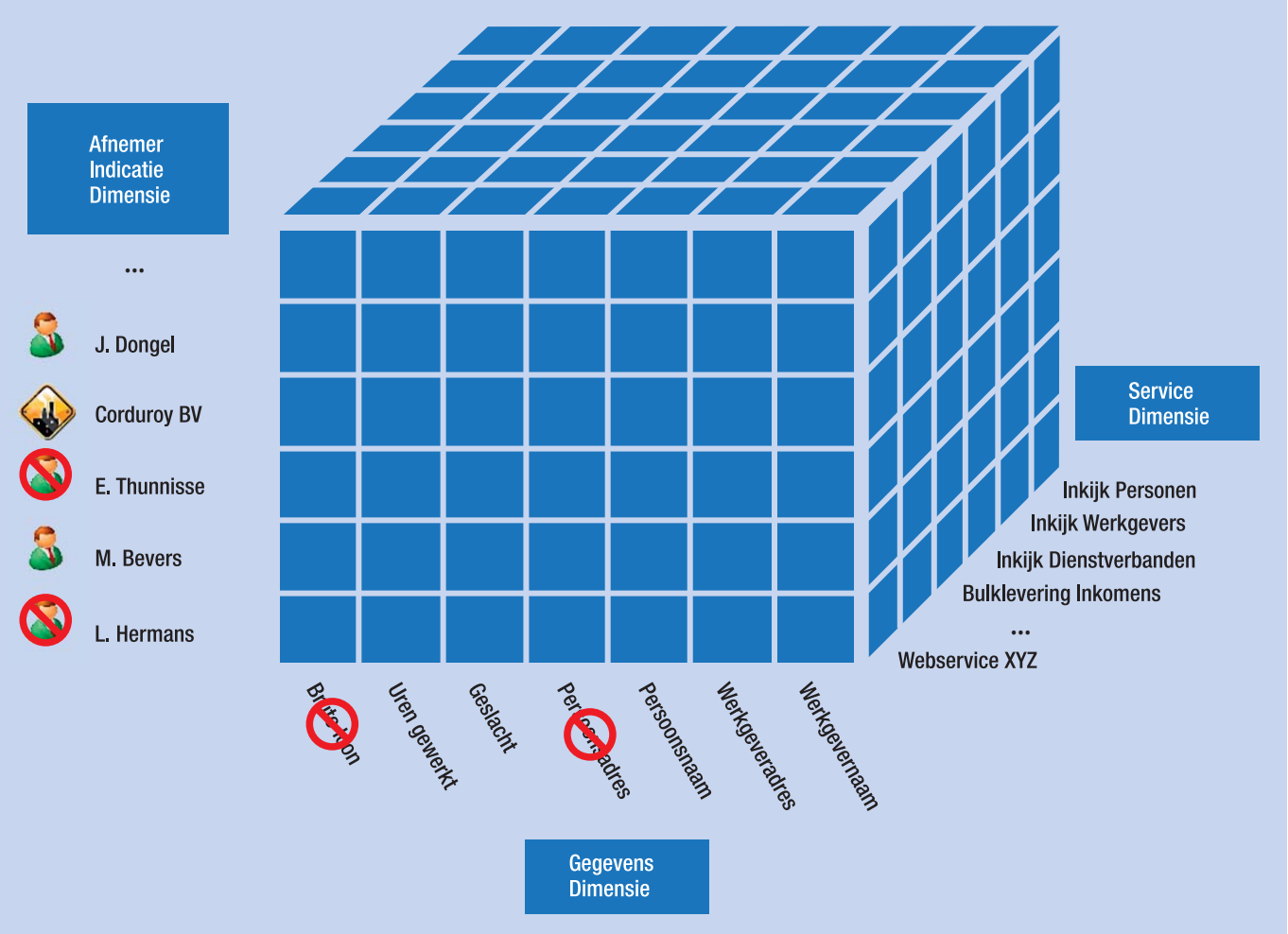
René Veldwijk en Henk Sweere

In de vorige artikelen introduceerden we de Polisadministratie als een databasetoepassing met een perfect geheugen en een extreme tolerantie voor het opslaan en verwerken van 'verkeerde' gegevens. Maar goed, fout of lelijk, alle inkomens- en persoonsgegevens in de PA zijn flink privacygevoelig en dat vraagt om een krachtig autorisatiemechanisme. De PA beschikt daarvoor over een voorziening die niet eens zozeer 'high-tech' maar wel 'high-concept' is. En ook hier verlegt de PA grenzen.

De PA heeft zich binnen één jaar na invoering al ontwikkeld tot een spil in de gegevenshuishouding van de BV Nederland. Nu al zijn de aantallen afnemers en de hoeveelheid geleverde gegevens fors. Terwijl de echte groei in gegevensuitleveringen nog moet komen, komt een ruwe schatting van de hoeveelheid in 2009 aan afnemers te leveren gegevens uit op ergens tussen de 1,5 en 2 Terabyte. En dat is uitgedrukt in zinvolle informatie, dus zonder de XML-opblaasfactor. Die omvang en groei is geen toeval maar beleid. De overheid streeft namelijk naar een samenhangend stelsel van basisregistraties (zie www.stelselvanbasisregistraties.nl) waarin de PA onder de naam BLAU een belangrijke rol inneemt. Basisregistraties staan niet los van elkaar. De loonaangifte bevat bijvoorbeeld gegevens van personen en bedrijven. Als afnemers van de PA persoonsgegevens nodig hebben dan wordt waar mogelijk teruggevallen op de officiële verzameling persoonsgegevens in de GBA. Wil men gegevens van bedrijven, dan wordt (nog) gebruik gemaakt van de Werkgeversadministratie (WGA) van de belastingdienst. Het eindresultaat is een gegevensbank die een zeer gedetailleerd beeld biedt van dienstverbanden en verdiensten van burgers en bedrijven in Nederland. De gegevens in de PA zijn een droom voor bedrijfsspionnen, marketeers, stalkers, informatiebureaus en de Marokkaanse geheime dienst. En op 70.000 mensen met een inkijkautorisatie zijn er vermoedelijk wel een paar mensen die willen weten hoeveel Katja S. verdient. Goede autorisatievoorzieningen zijn dus van het grootste belang, juist omdat het doel van een basisregistratie is om zoveel mogelijk partijen met legitieme vragen te bedienen. Een lekke basisregistratie is potentieel een nachtmerrie.

Hoe autorisatie werkt

Aansluiting op de PA gebeurt alleen op basis van een deugdelijke wettelijke grondslag. Gegevens mogen door een afnemer alleen worden gebruikt voor het wettige doel waarvoor ze zijn verstrekt. *Doelbinding* heet dat. Autorisatie begint dus bij de wetgever en wordt nader ingevuld door juristen van UWV en de afnemer. Daarna pas komen wij ICT'ers in beeld en meteen zien we ons dan gebonden aan twee concepten van automatisering die ten tijde van het 'oude' PA-systeem zijn ontwikkeld. Enerzijds is daar het idee van 'hard uitkrassen'. Webservices, *message queue* leveringen en bulkbestandsleveringen worden op basis van °°°specificaties gewoon geprogrammeerd. Vanuit autorisatieperspectief is dat perfect, want de autorisaties zijn ingebakken in de specificaties en de code. Maar tenzij de PA onderdeel gaat uitmaken van een kredietcrisis werkverschaffingsprogramma willen we dat natuurlijk niet, want elke leveringvariant vereist nu betrokkenheid van ontwerpers, programmeurs, testers, enzovoort. Anderzijds zijn er zogenaamde 'Generieke Gegevendiensten' (GGD's) bedacht die geïmplementeerd zijn als webservices. Die GGD's leveren steeds een vaste set gegevenselementen – vaak meer dan nodig voor de doelbinding. Dat betekent dat UWV strikt genomen moet controleren of afnemers gegevens die ze wettelijk niet mogen krijgen niet toch stiekem inzien. Dat kan natuurlijk niet en begrijpelijkerwijs worden de GGD's niet gebruikt voor leveringen aan externe afnemers. Er is met die GGD's nog iets anders aan de hand. Ze halen steeds één klasse van gegevens op: werkgevers, personen, inkomstenverhoudingen of inkomstenbedragen. Stel dat je de gegevens van een uitzendkracht wilt raadplegen die dertig baantjes heeft gehad, dan heb je als afnemer zomaar 62 ping-pong uitwisselingen met de PA: één voor het ophalen van de persoonsgegevens, één voor het ophalen van de verzameling inkomstenverhoudingen, dertig voor het ophalen van de inkomsten en nog eens dertig voor het ophalen van de werkgeversgegevens. Het moet anders, beter … En als we het beter doen dan moeten we meteen maar rekening houden met de noodzaak om 'horizontaal' te kunnen autoriseren. Veel afnemers mogen maar een deel van de populatie van de PA benaderen en de GGD's voorzien niet in een u-bent-niet-geautoriseerd-voor-sofinummer-123456789 melding. Dat knelt nog niet omdat de meeste huidige gebruikers van de GGD's in beginsel iedereen in de PA mogen



Afbeelding 1: De autorisatiekubus.

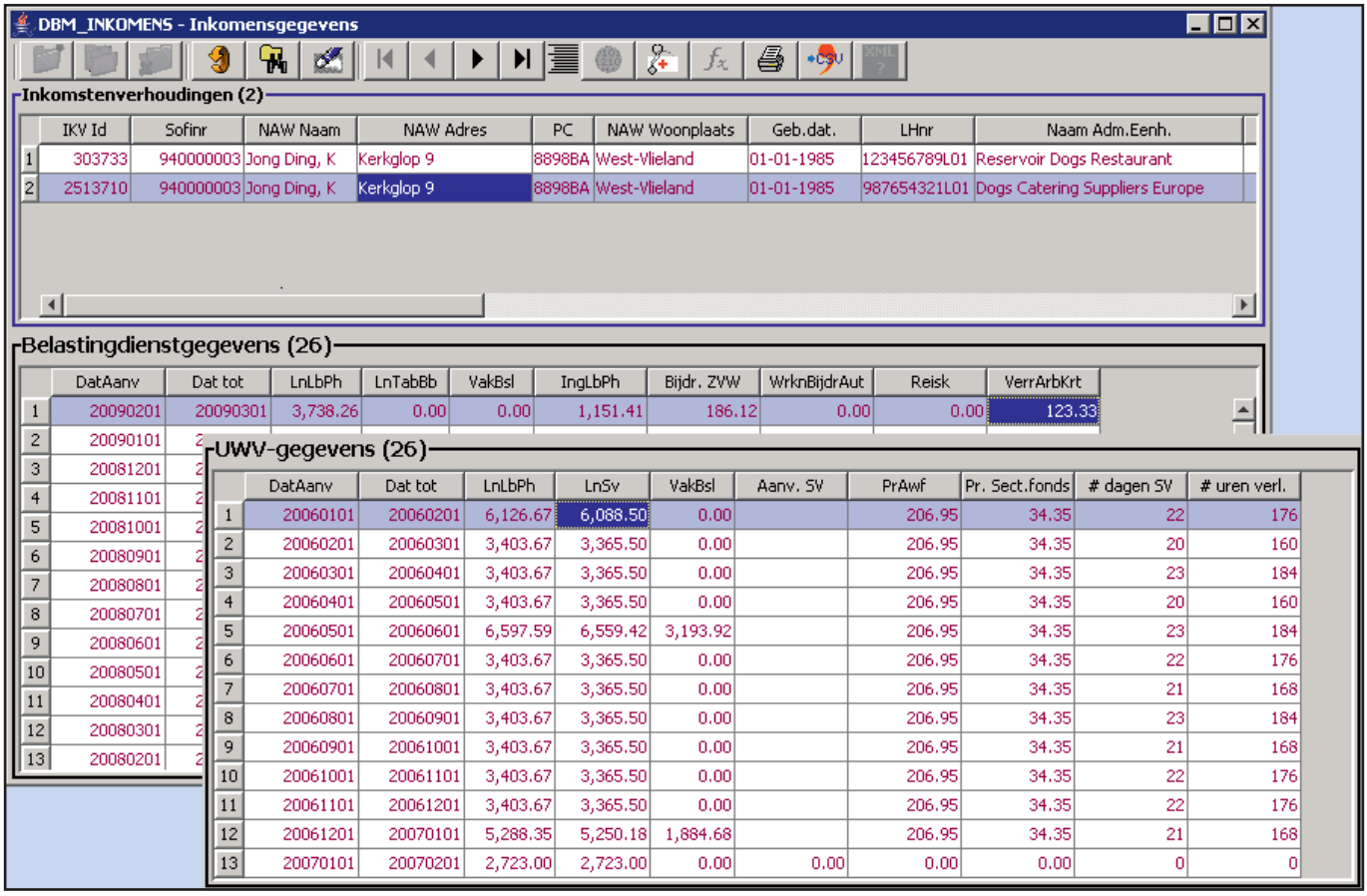
opvragen, maar erg duurzaam is het allemaal niet. De conclusie is dat de autorisatie voor dit moment goed is geregeld, maar op een manier die functioneel niet duurzaam en technisch niet schaalbaar is. De burger kan dus rustig gaan slapen maar de ICT-architect ligt er wakker van.

Autoriseren zonder automatiseerders

Precies zoals bij de uitdagingen die we in de vorige artikelen bespraken, kiezen we ook hier weer voor de radicale benadering. Autoriseren is wat ons betreft parametriseren en niet programmeren. Dat betekent dat programmeurs zich niets gelegen zouden moeten laten liggen aan autorisatie-overwegingen. We willen dus onder de software die gegevensleveringen verzorgt een generiek mechanisme leggen dat de autorisatie afhandelt op basis van door beheerders gedefinieerde parameters (die natuurlijk zelf ook weer onderworpen zijn aan een strenge autorisatie). Daarbij rafelen we alles dat betrekking heeft op autorisatie in drie onafhankelijke dimensies uiteen, zie afbeelding 1.

Die dimensies zijn: 1. de gegevenssoorten waarvoor afnemers zijn geautoriseerd; 2. de *services* die de afnemer mag gebruiken; 3. de deelpopulatie van personen en/of bedrijven waartoe de afnemer toegang krijgt. Het werken met onafhankelijke autorisatiedimensies leidt tot een hoog niveau van controle en maakt functiescheiding in de inrichting van de PA mogelijk. Controle ontstaat doordat het met een handjevol simpele instellingen mogelijk is om heel gericht autorisaties te verstrekken. Autoriseren op maat is dus altijd mogelijk en is snel en eenvoudig te regelen. De mogelijkheid van functiescheiding ontstaat door de strikte scheiding tussen de dimensies. Zo is het mogelijk om het parametriseren van de gegevenssoorten over te laten aan juridisch ingestelde beheerders en de autorisatie van services neer te leggen bij meer ICT-georiënteerde beheerders. Pas wanneer iedereen zijn autorisatiesleutel omdraait krijgt de afnemer gegevens te zien. Bij de inkijkschermen werken we al op deze manier. Wordt een afnemer/gebruiker geautoriseerd voor alleen het gebruik van een scherm, dan wordt een leeg scherm getoond. Wordt een afnemer/gebruiker geautoriseerd voor het raadplegen van, zeg, persoonsgegevens en inkomstenverhoudingen dan heeft hij nog niets want zonder toegang tot een service kun je niets beginnen. Maar combineer de autorisaties en je hebt functionaliteit op maat. Bijgaand twee keer hetzelfde scherm: één keer voor een UWV medewerker en één keer voor een functionaris van de Belastingdienst, zie afbeelding 2.

Afbeelding 2 laat zien hoe we uitgaande van een handjevol gestandaardiseerde schermtemplates verschillende groepen gebruikers



Afbeelding 2: Eén service, twee gegevensautorisaties.

kunnen bedienen met alleen de voor hun relevante gegevens. De functiepunten vliegen ons om de oren. Ook interessant is dat gegevens die door middel van een scherm zichtbaar zijn ook via een webservice kunnen worden aangeboden en omgekeerd. Stel dat onze juridisch aangelegde UWV-medewerker de gegevensautorisatie voor een afnemer heeft ingericht, het algemene inkijkscherm opent en ziet dat het goed is. Dan is impliciet meteen een deel van een (toekomstige) flexibele webservice al geparametriseerd. *Tsjakka!* Nu zitten we alleen nog met de vraag of het wel gewenst is dat voor een afnemer de gegevensinrichting van alle services altijd gelijk oploopt. Concreet: is het wel gewenst dat als we gegevens aan de deurwaarders leveren via een webservice, we precies dezelfde gegevens tonen wanneer we die deurwaarders een 'inkijkschermservice' zouden bieden? Ons antwoord op die vraag is JA. Sterker nog: als een afnemer vragen heeft over de geleverde PA-gegevens, dan behoort hij wat ons betreft eerst via een inkijkscherm na te gaan of hij bij het UWV moet aankloppen of bij zijn eigen ICT-collega's. Reken maar dat zoiets veel gedoe scheelt, vooral bij afnemers die gegevens uit de PA integreren met hun eigen gegevens.

De autorisatiekubus: 2/3 BUY en 1/3 MAKE

Hoewel het idee van onafhankelijke database-autorisaties niet compleet nieuw is, werken verreweg de meeste systemen op basis van een model waarin de functionele autorisatie (schermen, rapporten, webservices) leidend is en de database-autorisatie daarvan wordt afgeleid of gewoonweg ontbreekt. De PA is echter gebaseerd op het High~T dictionarymodel waarin deze autorisatiedimensies netjes zijn gescheiden. Maar gescheiden functionele en gegevensdimensies zijn onvoldoende. We missen nog een derde dimensie: de al genoemde horizontale autorisatiedimensie. Hier is dat de autorisatie van populaties van burgers en bedrijven. Wij zijn helaas niet slim genoeg om dáárvoor een werkelijk generiek, declaratief mechanisme te bedenken. Weliswaar beschikken we over een mechanisme waarmee we SQL-filters (*Where clauses)* kunnen toevoegen aan een database raadpleging, maar zo'n op expressies gebaseerd mechanisme is foutgevoelig en per definitie het domein van programmeurs. Daarom hebben we een declaratief mechanisme ontworpen dat generiek genoeg is voor de PA en misschien wel voor alle basisregistraties van de overheid.

We volgen hier de weg die de bevolkingsadministratie lang geleden heeft gewezen: die van de afnemerindicaties. Afnemers van de GBA verzoeken om een indicatie te plaatsen bij burgers in wie zij geïnteresseerd zijn. UWV doet dat zelf bijvoorbeeld voor alle nieuwe personen die de PA instromen, waarna de GBA eerst een geautoriseerde initiële gegevensset en daarna de relevante mutaties doorstuurt. De GBA werkt met slechts twee autorisatiedimensies: services/gegevenssoorten enerzijds en afnemerindicaties anderzijds. Conceptueel lijkt het allemaal echter sterk op elkaar, behalve dan

natuurlijk dat het mechanisme van afnemerindicaties bij de PA veel uitgebreider is. Om te beginnen kent de PA niet één maar drie aanhaakpunten voor afnemerindicaties: personen (net als bij de GBA) maar ook bedrijven en inkomstenverhoudingen. We kunnen het Shell pensioenfonds autoriseren voor de bedrijven in het Shell concern, waarna het pensioenfonds toegang heeft tot alle inkomstenverhoudingen van mensen die bij de Shell bedrijven werk(t)en. Natuurlijk kunnen we die toegang beperken tot vastgestelde tijdsintervallen. En ook kunnen we aangeven dat de ex-Shell medewerkers Bos en Bolkestein uitgezonderd zijn van raadplegingen, want afnemerindicaties mogen ook negatief zijn. Voor Wouter Bos is dat zelfs gegarandeerd het geval, want hij is een minister en gegevens over VIP's mogen we tijdelijk niet uitleveren. Dat wordt nog vervelend als Wouter straks 65 (of 67) wordt. Een bedrijfspensioenfonds zoals dat van Shell of Philips is snel klaar met autorisaties op werkgeverniveau, maar soms is het moeilijker. Een commerciële verzekeraar als Aegon moet bijvoorbeeld gericht afnemerindicaties kunnen plaatsen bij personen met wie een individuele pensioenverzekering is afgesloten. De PA ondersteunt het allemaal.

Autoriseren van autorisaties

Waar we bij die horizontale autorisaties een beetje gemakkelijk aan voorbij lopen is de vraag hoe UWV moet nagaan of een verzoek om een afnemerindicatie te plaatsen wel gerechtvaardigd is. Wie zegt ons dat iemand bij Aegon niet bezig is om indicaties te plaatsen bij BN'ers in opdracht van de Privé? Een deel van het antwoord op die vraag is goed autoriseren bij Aegon intern, maar natuurlijk moet er ook worden gecontroleerd. Bij dat laatste kan de PA weer helpen, want ook de vastlegging van afnemerindicaties is weer *total recall* (zie artikel 1 in DB/M 1). En uiteindelijk zijn er natuurlijk verschillende klassen van afnemers die verschillend moeten worden behandeld. Vermoedelijk komen we uit op *trusted* en *untrusted* afnemers, waarbij de *untrusted* afnemers wellicht weer zijn onder te verdelen in afnemers waarvoor UWV aangevraagde indicaties vooraf wil goedkeuren en afnemers waarvoor goedkeuring achteraf kan plaatsvinden. Het zal duidelijk zijn dat dergelijke fiatteringmechanismen nog moeten worden gebouwd, maar dat het de UWV-organisatie een hoop autorisatiewerk kan gaan kosten. Omdat we plaatsvervangend lui zijn hebben we daarom het idee gelanceerd om waar mogelijk mee te liften met andere basisadministraties, in het bijzonder de GBA. Als Aegon voor een verzekerde bij de GBA een indicatie mag plaatsen voor de ontvangst van verhuis- en overlijdensmutaties van hun klanten, waarom zou de GBA die indicatie dan niet meteen doorgeven aan de PA? Aegon en wij zijn dan in één klap klaar en mogelijk verbetert de kwaliteit en tijdigheid van de autorisaties. Het zal nog jaren duren, maar dit is het denken dat op termijn leidt tot een werkelijk *stelsel* van basisadministraties en tot substantiële lastenverlichting voor burgers en bedrijven (en omzetverlaging voor ICT-bedrijven).

Een pensioenfonds als dessert

We sluiten dit artikel af met een casus die laat zien hoe mooi autoriseren en het helpen van afnemers in elkaar kunnen grijpen. Die casus betreft een zogenaamd sectorpensioenfonds dat de pensioenen regelt voor alle mensen die werkzaam zijn in een bedrijfssector. Een slimme consultant die bezig was geweest met de oude PA, deed ze het idee aan de hand om de PA te gebruiken om greep te krijgen op de kruiwagen met kikkers die hun klanten zijn. Het gaat om ruim 30.000 bedrijven die komen en gaan en nogal eens 'vergeten' om de bij CAO verplichte pensioenpremies af te dragen. In de PA wordt echter per werkgever opgeslagen in welke bedrijfssector deze actief is en als die sector X is dan is het hun bedrijfstak. Met die informatie kan de PA volautomatisch afnemerindicaties op bedrijfsniveau plaatsen en verwijderen en relevante mutaties doorgeven aan het fonds. Het zal niet verbazen dat de 'dekkingsgraad' opeens met een paar duizend bedrijven omhoog schoot en de kosten van het napluizen van de Gouden Gids wegvielen. Nu stromen maandelijks de loonaangiften van honderdduizenden werknemers binnen om periodiek aan het fonds te worden uitgeleverd. Opeens hebben we een sluitende, geautomatiseerde gegevenshuishouding. Toch niet helemaal, het fonds kent een paar honderd 'buitenbeentjes': bedrijven die wel premieplichtig zijn maar niet onder de goede sector vallen. Die worden (nog) op aanwijzing van het fonds door UWV handmatig ingevoerd. Onvermijdelijk zijn er ook 'binnenbeentjes' en die geven we een negatieve autorisatie, zodat we over deze bedrijven niets uitleveren. En natuurlijk ging het recent fout toen er een bedrijf was waarvan de medewerkers *deels* bij het fonds zaten. Ook met een goede autorisatie-architectuur gaan er in de uitvoering dingen fout. Het verschil met een slechte architectuur is niet dat je problemen voorkomt of ze sneller oplost. Het verschil is wel dat je een probleem maar één keer hoeft op te lossen. *Case closed*.

De twee voorgaande artikelen werden enigszins in mineur afgesloten omdat we verder waren dan onze gegevensleveranciers en -afnemers. Hier ligt dat iets anders. Aan het autorisatiemechanisme wordt nog geschaafd en getimmerd, terwijl de programmatuur die we hebben ontwikkeld nog overwegend werkt op het 'programmeer-alles-uit model'. Ook het gebruik van horizontale autorisaties is nog beperkt, want de grote afnemers zijn instanties als Belastingdienst en CBS en die mogen bijna iedereen zien. En ook zijn er afnemers zoals het Inlichtingenbureau en minder bekende afnemers als CAK en LBIO die pseudo-eenmalig gegevens uitvragen en zich nog niet bewust zijn van de voordelen die het werken met afnemersindicaties biedt. Maar ach, dat komt allemaal op termijn wel goed.

Het volgende artikel behandelt de tegenvoeter van het generieke autorisatiemechanisme, namelijk het nog generieker loggingmechanisme van de PA. De Grote Broer die Polisadministratie heet bekijkt ons elke maand opnieuw. De vraag is daarom of er ook iemand bekijkt naar wie Grote Broer kijkt. We zullen zien.

René Veldwijk en **Henk Sweere** zijn partner bij FAA Partners, onderdeel van de Ockham Groep.