

Peter Waters

VN kiest voor Nederlandse i-pass

1. Uit een persbericht: New York, 18 maart 2027, 23.11 uur GMT

Alle lidstaten adopteren i-pass. Dat hebben de Verenigde Naties zojuist besloten.

2. Achtergrond

De keuze voor i-pass is een doorbraak na jarenlang gesteggel tussen VN-lidstaten. Vooral China en de VS opteerden voor hun eigen oplossingen.

Het idee voor i-pass komt uit Nederland. Na ontwikkeling en gebruik op nationale schaal volgde succes in Europa. Nu faciliteert i-pass probleemloze authenticatie en vrij personenverkeer in en tussen de gemeenschappen.

Eurocommissaris Maxime Verhagen is opgetogen. “Dit is een echte doorbraak. Hiermee komt een cruciale bouwsteen voor de internationale informatie-infrastructuur beschikbaar.” Verhagen wijst verder op verbeterde borging van privacy. Ook VNO/NCW voorzitter Tofik Dibi is enthousiast. Hij onderstreept het gemak. “Er is een frustrerende hindernis opgeruimd voor de spectaculaire groei van internettransacties met Afrika, China en India.” Plagend voegt hij eraan toe dat de overheid voortaan geen enkele uitvlucht meer heeft om facturen te laat te betalen.

Verhagen heeft in 2017 als minister van Economische Zaken, Landbouw & Innovatie zelf het initiatief genomen tot de ontwikkeling van i-pass. Een jaar eerder waren de politieke verhoudingen weer eens ingrijpend gewijzigd.

Het nieuwe kabinet ging serieus aan de slag met infrastructuur voor informatieverkeer. “Weliswaar zeggen we dat we met z'n allen werken aan de netwerksamenleving,” analyseerde Verhagen, “maar tegelijkertijd maken we feitelijk allerlei hulpmiddelen die diezelfde netwerksamenleving ontkennen.” Grote bekendheid kreeg het filmpje op YouTube waarin hij alle pasjes uit zijn portemonnee liet zien. “Geén van die pasjes,” constateerde hij, “kan ik voor meer dan één soort toepassing gebruiken.” Zijn verzuchting luidde: “Hoezo netwerksamenleving?” Verhagen herinnerde nog eens aan problemen met de chipcards voor openbaar vervoer en het elektronisch patiëntendossier. “Zulke specifieke oplossingen zijn allang geen ... oplossing meer!” Hij kondigde één voorziening aan voor elke transactie, publiek of privaat, nationaal of internationaal. “Want dan is pas sprake van een zinvolle informatie-infrastructuur.”

Voor een doorbraak zorgde Verhagen verder door de overheid zich te laten beperken tot voorwaarden voor i-pass. Daardoor ontstond een markt voor het authenticatiemiddel. “Nee,” maakte hij de Tweede Kamer duidelijk, “ik zie geen principiële reden waarom de overheid i-pass zou moeten ontwikkelen, uitgeven, enzovoort.” Op die manier rekende hij voor authenticatie af met het onderscheid tussen een burger- en een privaatdomein. “I-pass faciliteert willekeurige transacties. Daarvoor is natuurlijk wél flexibel maar helder onderscheid nodig van rollen.”

Eind 2017 kwamen de eerste i-passen in Nederland beschikbaar. Inmiddels is i-pass ook in geheel Europa niet meer weg te denken.

Kenmerkend voor i-pass is dat niet één of andere techniek, maar een zo algemeen mogelijk concept van authenticatie voorop staat. Dat maakt i-pass toekomstvast. Daarom kiezen nu de lidstaten van de Verenigde Naties er met vertrouwen vóór.

De rest van dit hoofdstuk omvat een vroege uitwerking van het idee voor i-pass. Die tekst inclusief afbeeldingen stamt alweer uit 2009.

3. Stelselschaal!

Ingewikkelde publieke taken als veiligheid voor kinderen, betaalbare en toegankelijke gezondheidszorg en schoner-en-groener kunnen onmogelijk meer door één enkele overheidsorganisatie

worden behartigd. Dat vergt samenwerking van vele organisaties, steeds vaker ook nog eens van binnen en buiten de overheid. Afhankelijk van aan te pakken deelvragen in wisselende samenstelling. Met andere woorden, partijen moeten als in een dynamisch netwerk met elkaar samenwerken. Aparte oplossingen voor één organisatie of voor een vast samenwerkingsverband zijn ongeschikt. Want wat bij de ene organisatie paste, doet dat niet meer bij een andere. De uitdaging is om oplossingen te ontwikkelen die voor het hele netwerk passend zijn. Ik noem dat stelselmatig.

U en ik hebben inmiddels tientallen identiteitspasjes en dat aantal groeit nog steeds. Nadeel is dat elk van die pasjes doorgaans maar voor één enkele transactiesoort geschikt is. Voor echte groei van digitale transacties, ook over de landsgrenzen heen, is deze aanpak daarom ongeschikt.

Het is mijn overtuiging dat echte samenhang, interoperabiliteit en daarmee gebruikersgemak en betrouwbaarheid pas ontstaan wanneer identificatie, authenticatie, autorisatie en mandatering op stelselschaal worden bekeken, dus niet elk vanuit een specifiek belang. Zo'n stelselbenadering moet dan voorts niet alleen naar de Nederlandse situatie kijken, maar meteen een internationaal perspectief kiezen. Transacties houden immers niet bij de landsgrenzen op.

Ik heb de stoute schoenen aangetrokken en een denkmodel opgesteld voor zo'n stelselmatige aanpak van authenticatie en autorisatie. Dit leidt als het goed is tot een kader voor een stelselmatige aanpak van authenticatie en autorisatie. Zo'n kader kan mijns inziens helpen om bij de doorontwikkeling van lopende projecten geleidelijk meer synergie te krijgen en heeft zo een standaardiserende werking.

In een vijftal stappen bouw ik een stelselmatig informatiemodel. De deelschema's die ik daarbij gebruik en tenslotte het contextueel semantisch overzichtdiagram zijn gebaseerd op Metapattern.¹ Dezelfde schematechniek is gebruikt bij eerdere onderzoeken inzake semantiek.²

De voordelen van deze aanpak zijn evident. Gestopt kan worden met ontwikkeling van specifieke, single-issue oplossingen. Voor een netwerkoverheid is dat geldverspilling. Met een stelselmatige (generieke) standaard wordt de domeinspecifieke aanpak (burgerdomein versus privaat domein) doorbroken. Veel dubbel werk wordt zo voorkomen.

De kansen voor het bedrijfsleven (ontwikkeling van nieuwe markten) zijn groot, ook omdat de noodzaak voor de overheid vervalt om eigen middelen te maken, uit te geven en te beheren. De lijn eHerkenning wordt krachtig ondersteund en de voorgestelde aanpak is principieel geschikt voor gebruik over landsgrenzen heen.

4. Verkrijgen van een identiteit

Personen

Een mens is een sociaal wezen. Hij of zij is niet alleen. Alleen kan een mens niet overleven. Zijn menszijn krijgt pas vorm en inhoud in relatie met anderen. Die relaties kunnen familiaal van aard zijn. Of groter: stam, clan. Of véél groter: staat.

Om de groep (familie, stam, clan, staat e.d.) in stand te houden zijn afspraken nodig. Afspraken over bijvoorbeeld verwantschap, bezit, rechten en plichten.

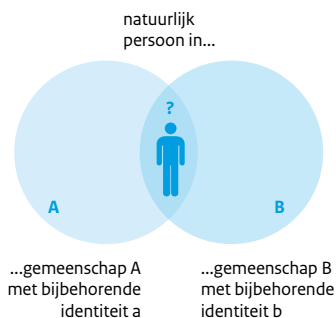
Voor het kunnen toewijzen van verwantschap, bezit, rechten en plichten moet de mens in persoon gekend zijn. Dat kenbaar maken in persoon noemen we *identificatie*: het aan een mens toewijzen van een identiteit.

¹ Met dank aan Pieter Wisse voor illustratie met informatiemodellen. Voor de toegepaste modelleermethode, zie zijn boek *Metapattern: context and time in information models* (Addison-Wesley, 2001) en de website *Metapatroon, handboek stelselmatig informatieverkeer* (Information Dynamics, www.informationdynamics.nl/handboekmetapatroon/)

² [http://www.forumstandaardisatie.nl/organisatie/documenten/publicaties/semantiek\(betekenisleer/\)](http://www.forumstandaardisatie.nl/organisatie/documenten/publicaties/semantiek(betekenisleer)/)

De meest simpele vorm van het toewijzen van een identiteit is het geven van een naam. In complexere samenlevingsvormen (organisaties) gebeurt dat met het vastleggen in een lijst of registratie.

Naarmate organisaties zich ontwikkelden werden rechten en plichten vastgelegd in wetten. Zo ontstonden soevereine organisaties, hierna aan te duiden als staten. Die wet- en regelgeving geldt bijna alleen voor het eigen rechtsgebied. Als gevolg daarvan kunnen rechten en plichten verschillen per territorium.



figuur 1: persoonsidentiteit per gemeenschap/organisatie.

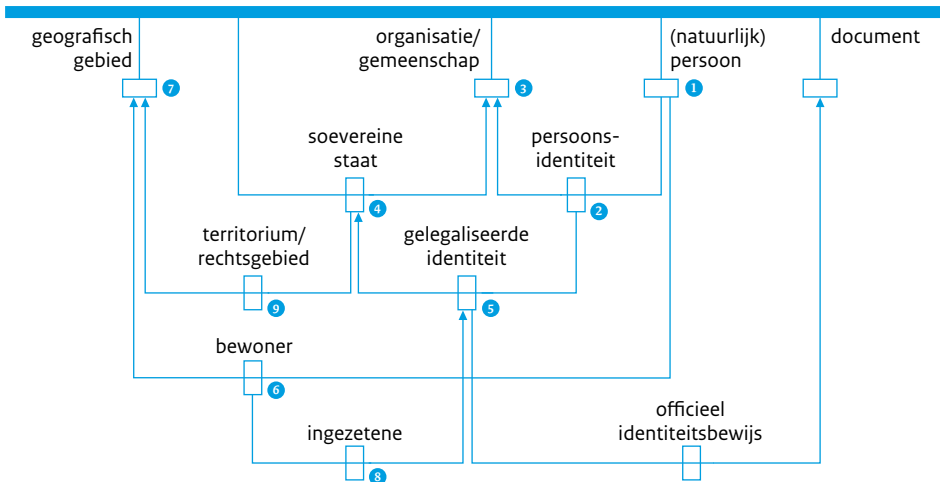
Om mensen als juridische entiteit te kunnen duiden worden ze verder aangeduid als *natuurlijk persoon*. Als regievoerder op maatschappelijke transacties houden staten voor hun rechtsgebied een lijst bij van natuurlijke personen die tot hun jurisdictie horen. Door opname van natuurlijke personen op die lijst krijgen die mensen een door de staat erkende identiteit.

Op basis van die toegekende identiteit kunnen ingeschreven natuurlijke personen ook identiteitspapieren krijgen die als een sleutel toegang geven tot publieke ruimten, maatschappelijke transacties en andere staten. Het paspoort is aldus de tastbare afbeelding van het proces van opname in een personenlijst. Op vergelijkbare wijze kunnen ook andere afbeeldingen worden gemaakt (identiteitskaart, rijbewijs of uittreksel uit het bevolkingsregister). Van belang is dat de verschillende afbeeldingen (identificatiemiddelen) verschillende doelen hebben en andere rechten en plichten met zich meebrengen. Met een rijbewijs kun je weer andere dingen dan met een identiteitskaart. Zie figuur 2.

Organisaties

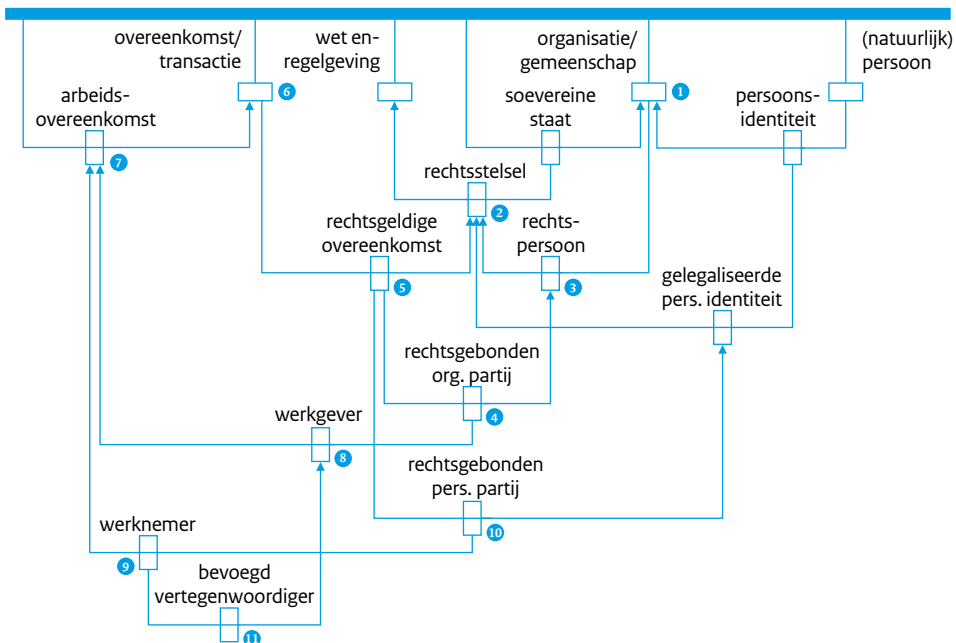
Mensen werken samen. Ze doen dat vaak in formele samenwerkingsverbanden. Door de soevereine staten kan aan die verbanden een vorm van rechtspersoonlijkheid worden toegekend. Dat biedt voordelen voor arbeidsdeling, schaalvergroting, verzamelen van kapitaal en beperking van risico. Ook hier is wet- en regelgeving leidend. Dat geldt voor de condities waaronder organisaties rechtspersoon kunnen worden, voor de spelregels waaraan transacties moeten voldoen en voor de rechten en plichten, verantwoordelijkheden en bevoegdheden, die daarmee worden opgebouwd respectievelijk toegewezen.

De vormen van rechtspersoon kunnen verschillen per soevereine staat. Ook de condities en spelregels kunnen verschillen per rechtsgebied. Maar altijd zullen het mensen zijn die als individu een organisatie in rechte binden en zo namens de organisatie rechten en plichten opbouwen. Zie figuur 3.



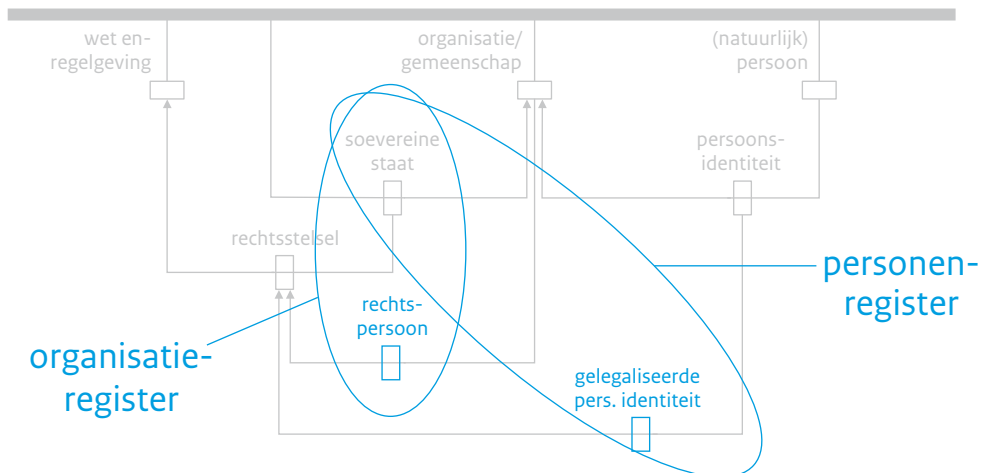
Een natuurlijk persoon ① ontleent een specifieke persoonsidentiteit ② aan, of krijgt haar toegekend door, een (sociale) gemeenschap respectievelijk organisatie ③. Indien die georganiseerde gemeenschap een soevereine staat ④ is, beschikt de natuurlijke persoon in kwestie daardoor zelfs over een gelegaliseerde persoonsidentiteit ⑤. Een natuurlijk persoon is bewoner ⑥ van een geografisch gebied ⑦, maar pas voorzien van een gelegaliseerde persoonsidentiteit telt hij daar als ingezetene ⑧. Nota bene, de soevereine staat die de gelegaliseerde persoonsidentiteit toekeende kan verschillen van de soevereine staat op wiens territorium/rechtsgebied ⑨ de persoon in kwestie als bewoner verblijft. Indien zulk verschil optreedt, geldt hij daar formeel als vreemdeling.

figuur 2: de ene persoonsidentiteit is de andere niet.

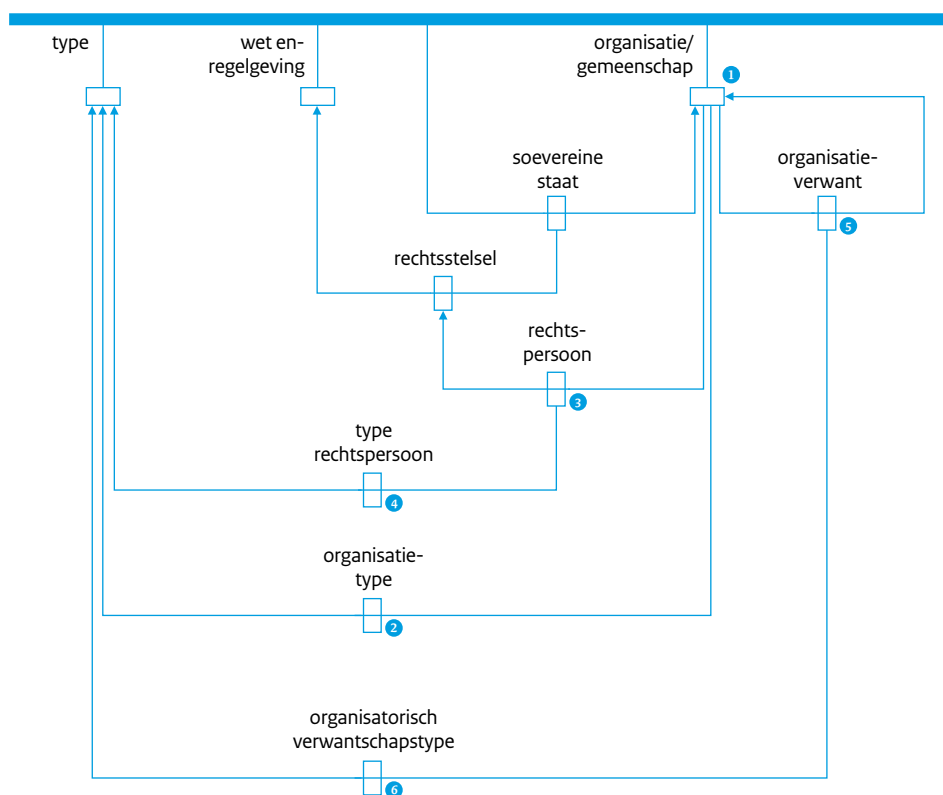


Een organisatie ① telt volgens een rechtsstelsel ② als rechtspersoon ③ en kan als zodanig rechtsgebonden organisatorische partij ④ zijn bij rechtsgeldige overeenkomst ⑤. Indien een overeenkomst ⑥ het karakter draagt van een arbeidsovereenkomst ⑦, is de rechtsgebonden organisatorische partij (zie 4.) in kwestie de betrokken werkgever ⑧, terwijl de werknemer ⑨ verwijst via de rechtsgebonden persoonspartij ⑩ naar een gelegaliseerde persoonsidentiteit (zie figuur 2). De werknemer kan eventueel optreden als bevoegd vertegenwoordiger ⑪ van de werkgever (zie 8.).

figuur 3: algemene 'spelregels' en nadere overeenkomsten met menselijke vertegenwoordigers.



figuur 4: positionering van (eventueel) personen- en organisatieregister per soevereine staat.



Een organisatie ① kan op haar algemeenst als een organisatietype ② ingedeeld zijn, maar ook in haar verschijningsvorm van rechtspersoon ③ kent zij eventueel een type rechtspersoon ④, terwijl tevens onderlinge relaties, dus organisatieverwant ⑤ van een organisatorisch verwantschapstype ⑥ kan zijn voorzien. Enzovoort.

figuur 5: organisaties enzovoort in soorten en maten.

In hoeverre ze persoonlijk aansprakelijk zijn voor die handelingen is in de spelregels omschreven. Ook organisaties hebben een identiteit. Met naam en adres en al. Daarin kunnen ook allerlei mutaties optreden. Gezien het belang van een betrouwbaar handelsverkeer worden de identiteitsgegevens van organisaties en de mensen die daarvoor verantwoordelijk zijn, in die hoedanigheid dus, eveneens bijgehouden in lijsten (registers). Zie figuur 4

Organisaties kunnen verschillende vormen kennen. Zoals bij mensen sekse en leeftijd bepalende onderscheidende factoren zijn, zo zijn bijvoorbeeld vorm van rechtspersoon en omvang dat bij organisaties. Een kerkgenootschap kent hele andere rechten en plichten dan een beursgenoteerde naamloze vennootschap, of een overheidsdienst.

Zoals opgemerkt worden de identiteitsgegevens van organisaties bijgehouden. Eén van de aspecten daarvan is organisatorische verwantschap. Denk maar aan het spraakgebruik waar we spreken over een moederbedrijf en een dochteronderneming. Bovendien wordt onderscheid gemaakt tussen verschillende locaties. Zie figuur 5.

Hoeveel identiteiten heeft een mens?

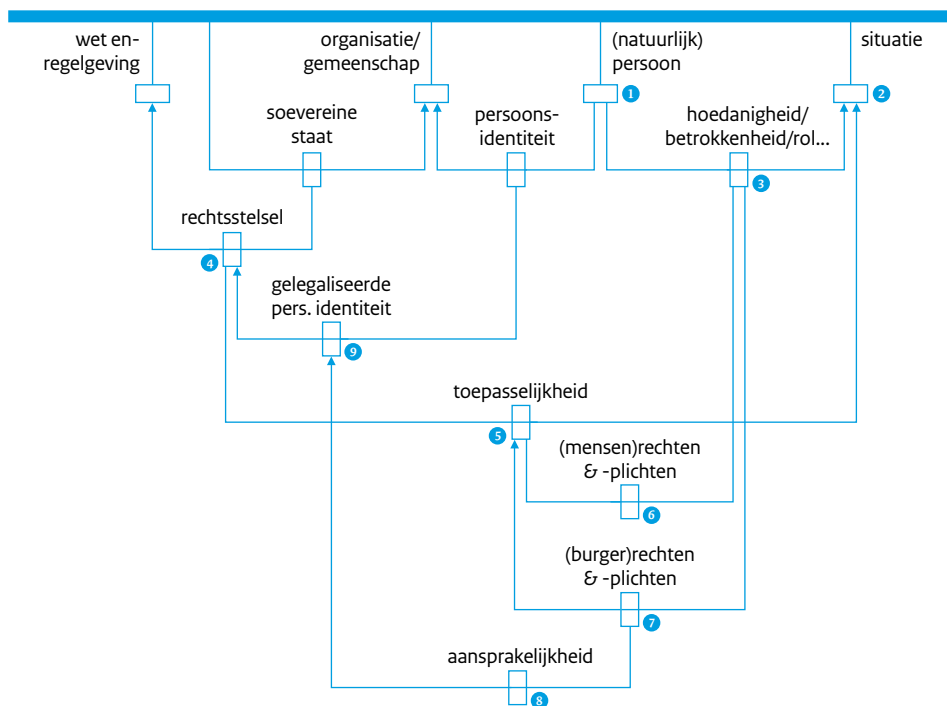
Mensen hebben minimaal één identiteit. Die krijgen ze toegewezen bij hun geboorte. Maar het kunnen er meer zijn. Soms omdat ze in meerdere jurisdicties zijn ingeschreven. Legaal of illegaal. Soms hebben ze in de digitale wereld zelfs een alias (avatar), waarmee ze ook weer rechten en plichten kunnen verwerven.

Omdat het niet realistisch is als universeel geldig uitgangspunt te hanteren dat een natuurlijk persoon slechts één identiteit mag hebben, geldt voor het stelselmatige informatiemodel dat iedereen één of meerdere identiteiten kan hebben. Dat is minimaal afhankelijk van het aantal wettelijk vastgelegde registraties waarin iemand als individu is opgenomen. Maar, let wel, met wat op een klantenkaart staat heeft de persoon ook 'een' identiteit, te weten voor de leverancier in kwestie.

Iedereen kan als persoon in een rechtsstaat meerdere hoedanigheden hebben. Hij kan niet alleen ingezetene zijn van een rechtsstaat, maar tegelijkertijd ook vreemdeling, ondernemer, bestuurder, werknemer, Eerste Kamerlid en lid van een golfclub. In elk van die hoedanigheden heeft hij dienovereenkomstige rechten en plichten.

Die hoedanigheden worden doorgaans *rollen* genoemd. Binnen elke identiteit kunnen rollen worden benoemd en toegewezen. Dat gebeurt ook weer in lijsten (registers). Alle rollen van een persoon of organisatie tot één identiteit beperken is (zoals boven aangetoond) niet realistisch. Voor betrouwbaar (her)gebruik is het echter praktisch wanneer informatie die in diverse registraties over eenzelfde persoon, organisatie e.d. opgenomen is, samenhang vertoont. Denk aan issues als het stapelen van subsidies en het voorkomen van fraude. Het leggen van die samenhang kan met expliciete verwijzingen, uiteraard slechts voor zover de wet dat toelaat.³ Zij die toegang hebben tot de informatie kunnen dan steeds zien dat transacties, rechten, plichten en rollen inderdaad aan dezelfde mens of organisatie zijn toegewezen. Zie figuur 6.

³ Zie hierover ook paragraaf 8, Privacy.



Het gedrag van een natuurlijk persoon ① in een maatschappelijke situatie ② valt onder de noemer van een rol ③. Wat van het rechtsstelsel ④ toepasselijk ⑤ is op de situatie in kwestie (zie 2), bepaalt in het algemeen de mensenrechten & -plichten ⑥ en in het bijzonder de burgerrechten & -plichten ⑦ van de gesitueerde persoon, dus in zijn rol (zie 3). De formele aansprakelijkheid ⑧ op gedrag verloopt via de gelegaliseerde persoonsidentiteit ⑨ volgens het geldige rechtsstelsel (zie 4).

figuur 6: zonder gelegaliseerde persoonsidentiteit geen formele aansprakelijkheid.

5. Authenticatie

In kleinere samenlevingsverbanden (tot ca. enkele honderden mensen) kennen mensen elkaar van gezicht en naam. Of weten tenminste tot welke familie hij of zij behoort.

Naarmate samenlevingsverbanden groter worden, wordt dat moeilijker. Je weet dan niet meer of iemand tot de eigen groep behoort; een vriend of vijand is. Of dat je iemand kunt vertrouwen bij het doen van transacties.

Naarmate samenlevingsverbanden groter worden en ook hun territorium, wordt het dus belangrijker dat mensen aan anderen die hen niet kennen, kunnen aantonen dat ze zijn wie ze zeggen te zijn. Identificatiemiddelen zijn daarvoor veel gebruikte instrumenten.

Het identificatiemiddel bevat informatie over de persoon. Dat is deels dezelfde informatie die in de eerder genoemde lijsten (registers) staan opgenomen. Voorzien van echtheidskenmerken om namaak en misbruik te voorkomen. Welke informatie en welke echtheidskenmerken dat precies zijn is afhankelijk van de afspraken die daarover zijn gemaakt. Voor de formele identificatiemiddelen van staten is dat vastgelegd in wetten.

Wanneer organisaties en/of staten over en weer identificatiemiddelen erkennen, kan een mens ook in een ander rechtsterritorium aannemelijk maken dat hij is wie hij zegt te zijn. Het paspoort is exemplarisch.

Het proces van het met een identificatiemiddel aantonen dat je bent wie je zegt te zijn, noemen we authenticatie. Dat kan live op straat gebeuren. Tussen twee personen.

Het kan ook online. Voor die authenticatie kun je een identificatiemiddel van een staat gebruiken⁴, maar ook andere organisaties kunnen identificatiemiddelen uitgeven. Let wel, je kunt ook zonder materieel identificatiemiddel de identiteit van iemand vaststellen. De relevante informatie over iemand wordt immers in de registers bijgehouden. Maar dat kost meer tijd. Met een identificatiemiddel gaat dat handiger.

Met technische middelen kunnen zeer betrouwbare identiteitswaarmerken aan een identificatiemiddel worden toegevoegd. De Europese Commissie onderscheidt daarbij vier betrouwbaarheidsniveaus. Bestaande identiteitsmiddelen kunnen in die classificatie worden ingeschaald.

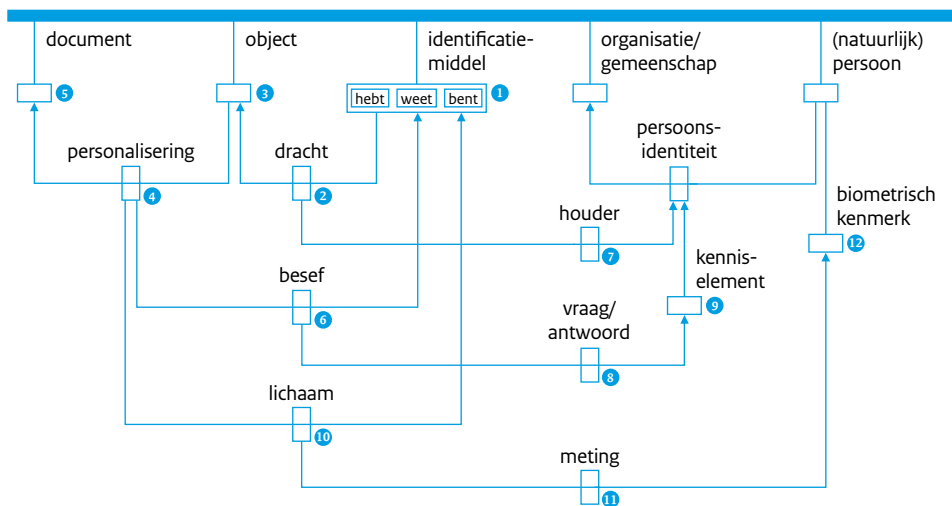
Voor de hogere betrouwbaarheidsniveaus wordt altijd een relatie gelegd met de informatie uit een basisregistratie. Die registers worden immers vaker geactualiseerd dan het identificatiemiddel zelf.⁵ Anders dan sommige politici menen is het dus in het algemeen belang dat banken toegang hebben tot (een deel van) de informatie in de GBA.⁶ Alle transacties met de identificatiemiddelen van banken worden dan veiliger. Dat leidt tot meer vertrouwen. Tot voordeel van iedereen.

In het vervolg van dit artikel zoom ik in op de digitale authenticatie. Maar principieel is er geen verschil met de herkenning live op straat. Zie figuur 7.

⁴ In Nederland hebben we dat nog niet, in andere landen, bijvoorbeeld Estland, België en Oostenrijk, bestaat dat wel.

⁵ Specialisten van Nederlandse banken melden dat de helft van de kwaliteit van een identificatiemiddel bepaald wordt door de kwaliteit van het middel zelf. De andere helft door de kwaliteit van het uitgifteproces. Dat lijkt zeer aannemelijk. Als de uitgifte procedureel niet goed wordt afgehandeld neemt de kans dat mensen frauduleus transacties kunnen uitvoeren sterk toe. Fraude ondergraaft het vertrouwen.

⁶ Gemeentelijke Basisregistratie Persoonsgegevens. In deze basisregistratie zijn de persoonsgegevens opgenomen van alle Nederlandse ingezetenen.



Een identificatiemiddel (lees ook: authenticatiemiddel) ❶ 'bestaat' uit dracht ❷ van een (im)materieel object ❸, eventueel voorzien van personalisering ❹ tot een (im)materieel document ❺. Zodoende kan authenticatie (tevens) rusten op besef ❻; de houder ❼ (lees ook: drager) geeft correct antwoord ❸ op een gerichte vraag naar een kennis-element ❾. En/of op het lichaam ❿ van de houder (zie 7.) als natuurlijk persoon gebeurt ter authenticatie een meting (en vergelijking) ❶ van een biometrisch kenmerk ❷.

figuur 7: de 'media-mix' voor authenticatie.

Bij gebruik van een identificatiemiddel om authenticatie te kunnen uitvoeren wordt de mate van zekerheid dat iemand daadwerkelijk is wie hij zegt te zijn bepaald door de betrouwbaarheid van verschillende componenten: de borging in een basisregistratie, de kwaliteit van het uitgifteproces en de kwaliteit van het identificatiemiddel zelf.

Zie dat de informatierelatie in figuur 7 principieel symmetrisch is: de burger maakt zich bekend naar de overheid toe, maar omgekeerd de overheid ook naar de burger. De burger moet immers eveneens kunnen verifiëren, in zijn geval of de overheid inderdaad degene is die deze beweert te zijn. Verder is symmetrie een noodzakelijke voorwaarde voor machine-to-machine communicatie.

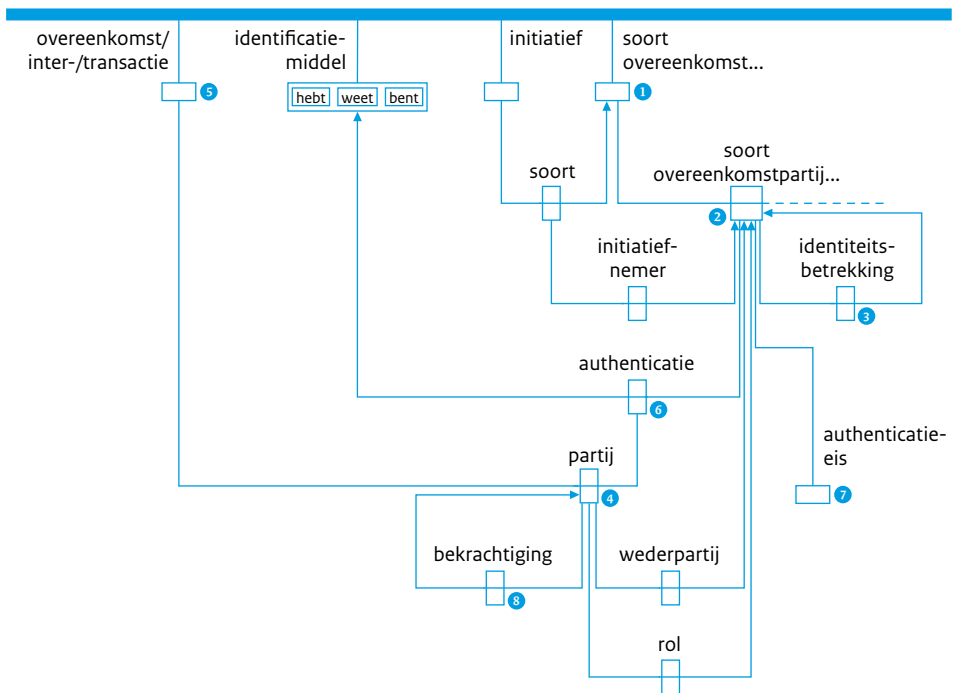
6. Autorisatie

Authenticatie is dus het vaststellen met behulp van een identificatiemiddel of iemand is wie hij zegt te zijn. Niet meer en ook niet minder. Niemand zal immers accepteren dat je door het simpele inloggen in een systeem meteen ook eigenaar van een mobiel telefoonabonnement bent geworden en daarvoor moet betalen. Dat geldt ook voor een belastingaangifte, het opleggen van boetes, het toekennen van een subsidie of het in het huwelijk treden met je partner. Dat vergt extra stappen.

Onder de noemer autorisatie wordt een viertal functies bekeken die voor het formeel afsluiten van transacties extra nodig zijn bovenop authenticatie: a. bekrachtigen voor en door jezelf, b. toewijzen van rollen (persoonlijk en in organisaties), c. toegang tot functies in systemen en d. digitale handtekening.

ad a. Bekrachtigen door en voor jezelf

Op de veemarkt was het gebruikelijk dat koper en verkoper na de onderhandelingen met handslag over en weer de verkoop bekrachtigen. Ze kenden elkaar vast al. Maar nu was voor iedereen zichtbaar dat de koop was gesloten. Dat hoeft dus niet schriftelijk. Handslag is wederzijds bindend en onherroepelijk.



(Verkeers)regels verkrijgen algemenere strekking dankzij classificatie. Zo kunnen allerlei (mogelijke) overeenkomsten gegroepeerd zijn als een soort overeenkomst 1 met voor elk kenmerkende soorten overeenkomstpartij 2 die voor het soort overeenkomst in kwestie een kenmerkende identiteitsbetrekking 3 kennen, resp. moeten aangaan. Daarvoor moet elke feitelijke partij 4 die deelneemt aan een feitelijke overeenkomst 5 met authenticatie 6 voldoen aan een bepaalde authenticatie-eis 7. Als dat gebeurt, geldt dat voor zó'n partij tevens als bekrachtiging 8 van de overeenkomst (zie 5).

figuur 8: een overeenkomst houdt een betrekking in tussen partijen, met karakteristieke (wederzijdse) authenticatie-eisen.

Van belang is dat mensen ook in een digitale omgeving na herkenning een volstrekt heldere extra handeling moeten verrichten. Door die extra handeling is de transactie bekrachtigd en onherroepelijk geworden. Een voorbeeld van hoe dat kan werken met een bankpas is IDEAL. Bekrachten gebeurt daar met een door de bank verstrekt authenticatiemiddel waarmee door een bewuste herhaling van de inlogprocedure de transactie digitaal wordt bekrachtigd. Zie figuur 8.

ad b. Toewijzen van rollen

Een *rol* wordt door Wikipedia gedefinieerd als “een standaard verzameling van taken, rechten en plichten voor een persoon binnen een bepaald domein.”

Ik ben met mijn vrouw in gemeenschap van goederen getrouwd. Door mijn huwelijk met haar heeft ze de rol van partner verworven (ikzelf trouwens ook). In die hoedanigheid kan zij mij (zelfs zonder overleg) in rechte binden.

Huwelijk brengt dus expliciet een rol voor de partners met zich mee. Zonder tegenmaatregelen (huwelijkse voorwaarden) zijn partners volledig mede aansprakelijk voor de gevolgen van transacties. Zij zijn ook verantwoordelijk voor letselschade die door hun minderjarige kinderen wordt veroorzaakt. Zij kunnen tenslotte in rechte aangesproken worden op nalatigheid in hun zorgplicht voor hun minderjarige kinderen.

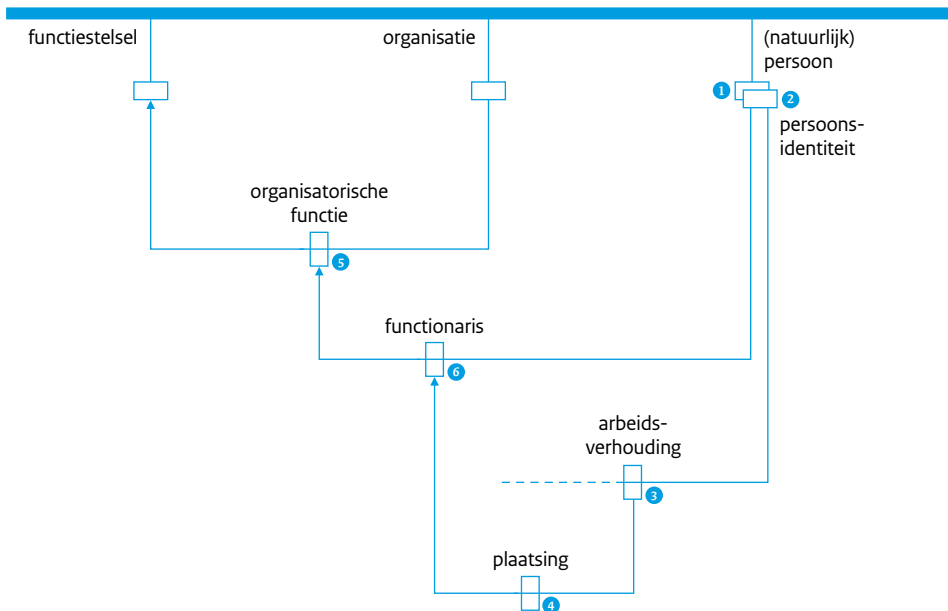
Het krijgen van kinderen (inclusief stief- en adoptief kinderen) brengt dus rollen met zich mee. Ik ga dan even niet in op complicaties zoals het toewijzen van voogdij of het uit de ouderlijke macht ontzetten. De wijze van verwerven of toewijzen van rollen aan verwanten (en daarmee bezit, rechten en plichten) is in het Burgerlijk Wetboek tot in de finesses vastgelegd. Voor zulke persoonlijke rollen is van belang dat een ieder op enig moment kan vaststellen welke rollen aan iemand zijn toegewezen dan wel afgenomen. Er zit immers een tijdsdimensie aan. Deze persoonlijke rollen kun je krijgen maar ook weer kwijtraken. Denk aan overlijden, echtscheiding en dergelijke.

Intermezzo: rollen in organisaties

Als ik een eigen zaak begin en medewerkers in dienst neem, zal ik hen taken (functies) toewijzen. Ik krijg er een rol als werkgever bij; de medewerkers die van werknemer. Uit de aard van hun functie zijn zij functionaris. Als functionaris kan ik hen nadere taken en rollen toewijzen. Op basis van die taken en rollen zullen sommige functionarissen mijn organisatie in rechte kunnen binden. Zij doen dat namens de organisatie. Transacties die voortvloeien uit die rollen zijn bindend en onherroepelijk.

Om betrouwbaar maatschappelijk (handels-)verkeer te kunnen borgen is van belang dat ook anderen de verantwoordelijkheden en bevoegdheden van mijn medewerkers in hun specifieke rollen kunnen kennen. Die toedeling van verantwoordelijkheden en bevoegdheden zal vaak getrapd zijn. Daarnaast speelt een aspect als functiescheiding.

Van belang is dat een medewerker in een organisatie meerdere functies tegelijk kan hebben en daarmee dus ook meerdere taken en rollen. Iemand kan tegelijkertijd lid van het management van een organisatie zijn, afdelingschef met lijnverantwoordelijkheid, lid van een projectteam en lid van een externe adviesraad. De context van die rollen is daarmee cruciaal. Zie figuur 9.



Een natuurlijk persoon **1**, bekend met een bepaalde persoonsidentiteit **2**, kent met één of meer werkgevers (in deze figuur niet getoond) een arbeidsverhouding **3**. Door plaatsing **4** in een organisatorische functie **5** geldt de persoon in kwestie als functionaris **6**.

figuur 9: gelijktijdig en/of achtereenvolgens verschillende (arbeids)plaatsingen tot steeds dienovereenkomstige functionaris.

ad c. Toegang tot functies in systemen

Wanneer werkzaamheden met een informatiesysteem ondersteund worden zullen rollen ook in dat systeem worden vastgelegd. Iedere rol geeft recht op toegang tot het systeem (of meerdere systemen). In dat systeem is de medewerker vanwege de rol bevoegd tot het doen van één of meerdere taken. Anderen zijn daarvan uitgesloten.

Van belang is te onderkennen dat rollen dynamisch zijn. Ze kunnen worden toegewezen, verval- len en qua inhoud veranderen in de tijd. Rollen zijn dus nooit absoluut. Wanneer een medewerker ontslag neemt is het verstandig de toewijzing van een rol aan die medewerker uit het systeem te verwijderen. Vanwege de veranderbaarheid van de rollen is het voorts verstandig de toewijzing van rollen decentraal bij te houden.

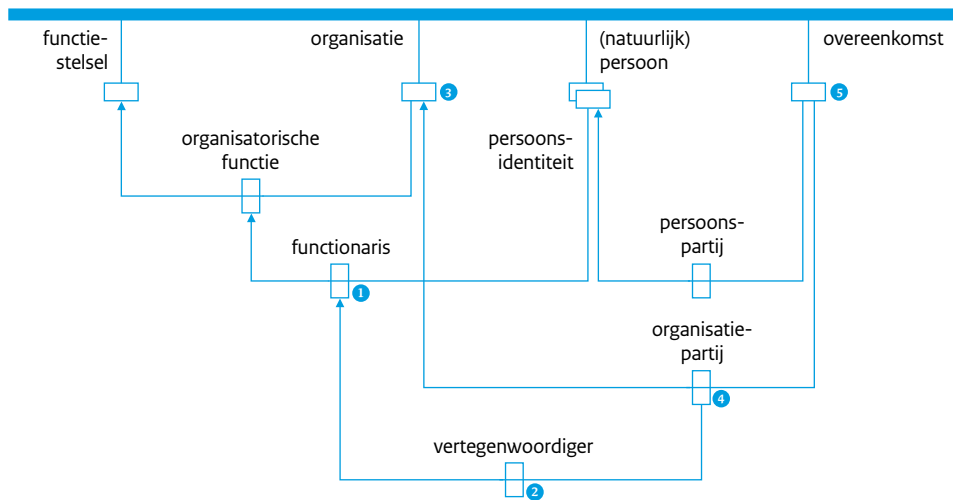
Wanneer een persoon meerdere rollen in meerdere systemen heeft, is het praktisch wanneer hij die in samenhang krijgt gepresenteerd. Een mooi voorbeeld is hoe men dat in Estland met een portal heeft ingericht. Wie daar inlogt in de portal van de overheid krijgt allereerst de vraag: komt u als burger of als ambtenaar? Wanneer je kiest 'als ambtenaar,' geeft het systeem vervolgens aan tot welke van de aangesloten systemen je bent toegelaten, in welke rollen en dus ook voor elke taken.

Dat doen ze via een register van registers, RIHA, dat real-time, online die informatie verzamelt en weergeeft.⁷

ad d. Digitale handtekening

Zoals aangegeven kunnen medewerkers op grond van de hen toegewezen rol hun organisatie onherroepelijk in rechte binden. In het klassieke verkeer is een handtekening onder een contract het bewijs dat de opdracht formeel is gesloten. Vaak staat daar dan ook de functie (rol) bij van de persoon die daarvoor eindverantwoordelijk draagt. Ook wanneer de transactie feitelijk door medewerkers lager in de organisatie is gesloten. Voor het maatschappelijk verkeer is het dus van belang dat de functionaris aan wie formeel de taak is toegewezen de transactie bekrachtigt. Met zijn handtekening maakt hij zichtbaar dat hij zich namens zijn organisatie gebonden acht.

Zoals eerder betoogd is bekrachtigen een extra handeling bovenop authenticatie. In de praktijk kan dat betekenen dat medewerker x met zijn persoonlijk identificatiemiddel een digitale handtekening plaatst, maar dat in de beschikking de naam en functie van de eindverantwoordelijke staat. Op basis van die digitale handtekening kan de eindverantwoordelijke wel herleiden wie de transactie feitelijk gesloten heeft. Zie figuur 10.



Een functionaris **1** treedt op als vertegenwoordiger **2** van de organisatie **3** die als organisatiepartij **4** betrokken is bij een overeenkomst **5**.

figuur 10: wie vertegenwoordigt/bindt de organisatie?

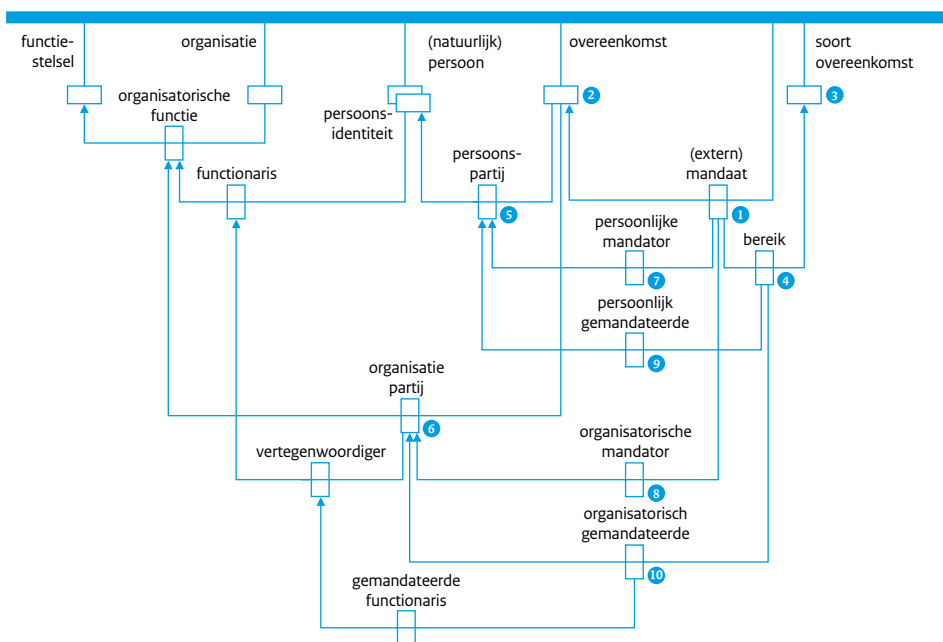
⁷ <http://www.ria.ee/27313>

7. Mandatering

Onder het kopje autorisatie kwamen de belangrijkste aspecten langs rondom herkenning van een persoon of organisatie, de wijze waarop rollen worden toegekend, de wijze waarop vanuit specifieke rollen toegang kan worden verleend tot transacties en hoe die transacties bekrachtigd kunnen worden. Getoond is hoe dat zowel transacties in de persoonlijke levenssfeer betreft als binnen de eigen organisatie.

Wat is nu extra nodig om een eventuele tussenpersoon niet behorend tot de eigen familie of eigen organisatie namens mij of mijn organisatie met een andere persoon of organisatie transacties af te laten sluiten?

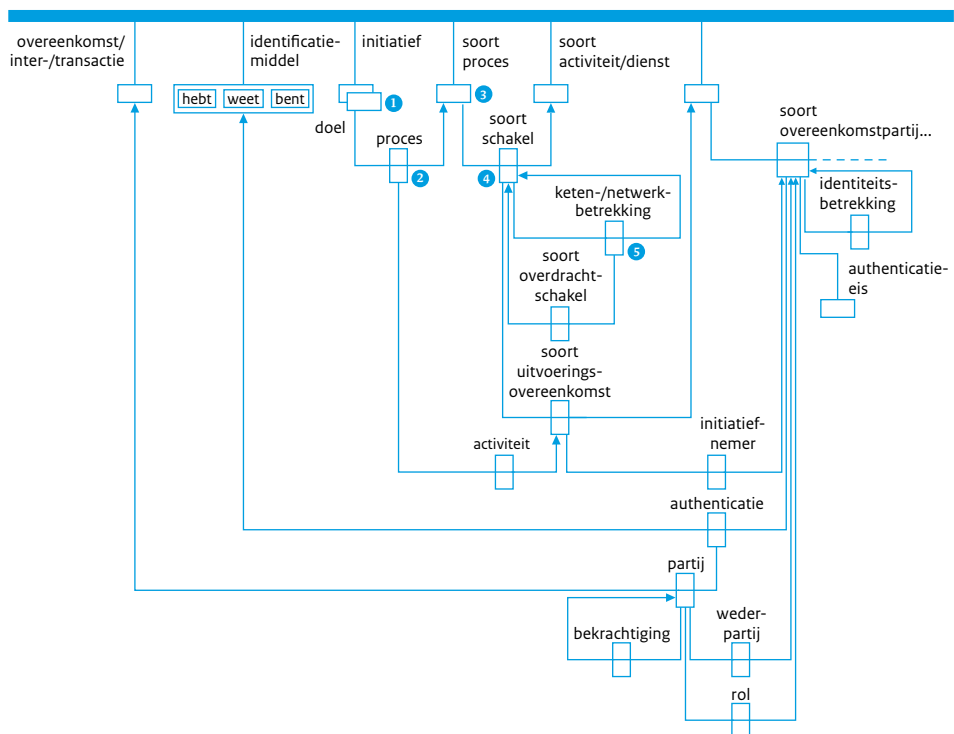
Vertrouwen is cruciaal in transacties. Van belang is dus dat voor iedere betrokkene helder is in welke rol die tussenpersoon (of organisatie) die transactie voor mij of mijn organisatie verricht. En ook dat die rol door die andere organisatie/persoon wordt erkend en de tussenpersoon in die



Een extern mandaat ① kan worden beschouwd als een overeenkomst ②, waarbij de indeling als soort overeenkomst ③ het bereik ④ van het mandaat bepaalt. Algemeen beschouwd heeft een overeenkomst (zie 2.) als deelnemers persoonspartijen ⑤ en/of organisatiepartijen ⑥. Indien een persoon het (extern) mandaat (zie 1.) verleent, is dus de betrokken persoonspartij (zie 5.) de persoonlijke mandator ⑦. Anders is de betrokken organisatiepartij (zie 6.) de organisatorische mandator ⑧. Dezelfde indeling is van toepassing op wie het mandaat kan uitoefenen, te weten een persoonlijke gemandateerde ⑨ die (dus) als persoonspartij aan het extern mandaat als overeenkomst deelneemt, of een organisatorisch gemandateerde ⑩ die (dus) organisatiepartij is.

figuur 11: een (extern) mandaat is een soort overeenkomst ...

rol wordt geaccepteerd. Tenslotte dat het voor die andere organisatie/persoon volstrekt helder is dat zowel ik als de tussenpersoon de transactie bekrachtigt. Dat kan structureel (de tussenpersoon doet voor mij een reeks transacties) of incidenteel. De eigenaar van het werkproces (Belastingdienst, een bank, een ziekenhuis, commercieel bedrijf) zal per werkproces helder moeten maken welke rollen het van tussenpersonen accepteert. Vervolgens kunnen tussenpersonen voor die benoemde specifieke rollen worden erkend en geaccepteerd. Dat kan betekenen dat een tussenpersoon door de Belastingdienst wel wordt erkend als belastingconsulent voor de inkomstenbelasting, maar niet voor de omzetbelasting. Opnieuw, de context van rollen is dus cruciaal. Zie figuren 11 en 12.



Dit is een uitbreiding van figuur 8 in de 'richting' van werkstroom e.d. Iemand neemt initiatief ① voor een proces ②. Indien dat de keuze voor een soort proces ③ inhoudt, is het verloop ervan wellicht à la keten of netwerk georkestreerd, dus met de ene (soort) schakel ④ in een gestructureerde keten-/netwerkbetrekking ⑤ met één of meer andere (soorten) schakels.

figuur 12: convergentie van overeenkomsten in werkstroom, met steeds dienovereenkomstige authenticatie-eisen.

Voor 'mijn' transacties is het van belang dat zowel ikzelf als de tussenpersoon de transactie bekrachtigen. Het is de regisseur van het proces (in dit voorbeeld de Belastingdienst) die het overzicht moet bijhouden van rollen en erkende tussenpersonen. Gezien de dynamiek en de variëteit van rollen en transacties verdient zo'n overzicht een decentrale opzet. Wel kan (vergelijk het voorbeeld uit Estland)⁸ online een dynamisch overzicht worden samengesteld op basis van de actuele decentrale informatie. Nogmaals, cruciaal is dat consequent en structureel telkens aangegeven wordt in welke context die rol geldt, wat de betekenis er van is en wat dat in transacties betekent. Daaruit volgt dat juist een 'centrale' rol is weggelegd voor semantiek.

8. Privacy

In de vierde paragraaf, Verkrijgen van een identiteit, hebben we gezien dat identificatie is ontstaan vanuit de behoefte om mensen (en organisaties) te kennen en om daarmee verwantschap, bezit, rechten en plichten te kunnen toewijzen. Deugdelijke vastlegging van die informatie en daarmee van identificatie is al millennia een noodzakelijke voorwaarde gebleken om grotere samenlevingen in te richten en in stand te houden en om betrouwbaar maatschappelijk- en handelsverkeer in te richten.

Waarschijnlijk ook vanaf het begin is er een spanning tussen de belangen van het collectief versus het individu. Het is aan de politiek om die soms tegenstrijdige belangen tegen elkaar af te wegen. Een wenkend perspectief voor de afweging van die belangen levert het Manifest voor informatieverkeer⁹ dat enerzijds de eigendom van persoonsinformatie principieel bij de burger legt, maar tegelijk de mogelijkheid open laat om daar waar het algemeen belang dat vereist dat wettelijk anders te regelen.

Daarmee is eigenlijk meteen de vraag over de eigendom van identiteitsgegevens in basisregistraties beslecht. Deze ligt bij de burger, of bij een bedrijf. Maar de wetgever kan besluiten om de eigendom van of, liever gezegd, de beschikking over delen van de identiteitsgegevens bij wet neer te leggen bij de overheid. Dat kan alleen met instemming van het Parlement. Dat gebeurt ook in de praktijk. De registraties worden immers vanuit een algemeen belang aangelegd. Niet vanuit een particulier belang van een individu of organisatie. Namens de samenleving ontwikkelt en beheert de staat die registers. Dat beheer moet de staat dan ook inrichten vanuit het besef van dat algemeen belang: betrouwbaar en controleerbaar. Burgers zijn immers kwetsbaar als er vanuit specifieke belangen vrij en oncontroleerbaar met hun informatie wordt omgegaan. Toegang tot en gebruik van de informatie moet strikt gereguleerd zijn. Vertrekpunt bij het toewijzen van gebruiksrechten moet gebaseerd zijn op een aantoonbaar algemeen belang. Anders kun je als burger geen vertrouwen hebben in het stelsel van registraties.¹⁰

Zolang ik als burger geen weet heb van de informatie die over mij is vastgelegd, geen mogelijkheid heb om te controleren of die informatie klopt en wat er mee gedaan wordt kan ik niet echt vertrouwen hebben in de overheid die dat allemaal opzet.

Een noodzakelijk voorwaarde voor vertrouwen zal daarom ook zijn dat ik (mits met identificatiemiddelen goed beveiligd) te allen tijde mijn informatie in kan zien, fouten eenvoudig kan melden, er op kan vertrouwen dat de overheid die foutmelding serieus in behandeling neemt en kan zien

⁸ Zie paragraaf 6c.

⁹ Voor genoemd Manifest, zie het volgende hoofdstuk in deze bundel.

¹⁰ Anders ligt dat bij identiteitsgegevens die door het bedrijfsleven worden verzameld en bijgehouden. Denk als voorbeeld aan de Bonuskaart van Albert Heijn. Het Manifest voor informatieverkeer doet interessante voorstellen hoe daar mee omgegaan kan worden. Maar dat is buiten de scope van dit hoofdstuk.

welke (overheids)organisaties op welk moment mijn informatie hebben geraadpleegd of gebruikt zo mogelijk voorzien van de context waarin die informatie is geraadpleegd.¹¹ Dit laatste uiteraard met uitzondering van recherche en veiligheidsonderzoeken, mits op wettelijke grondslag.

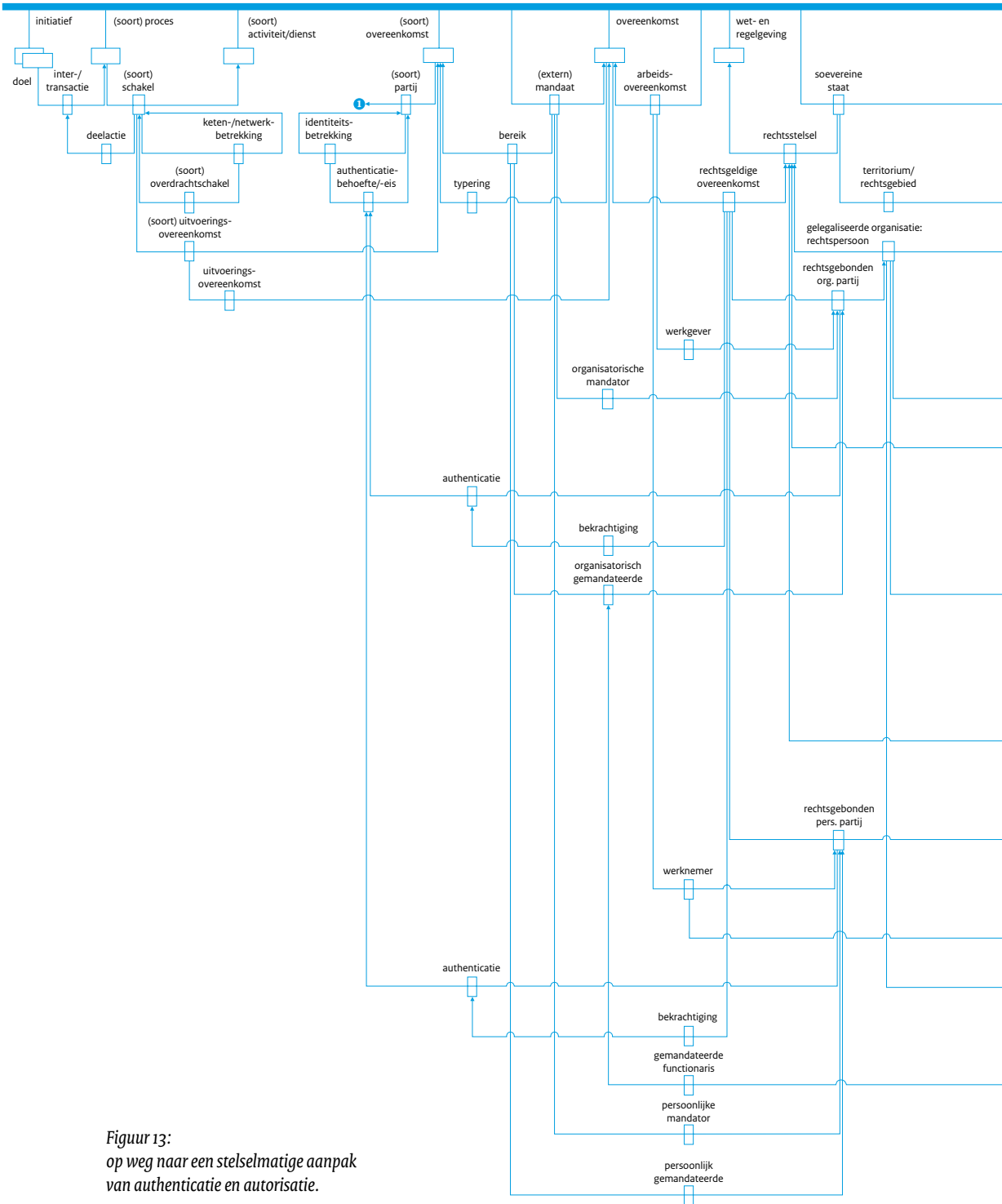
Opnieuw is Estland een mooi voorbeeld. Als een ingezetene zich daar als burger bij de overheidsportal meldt, toont het systeem (via het register van registers RIHA) in welke bestanden informatie over hem, zijn partner en minderjarige kinderen zijn opgeslagen. Die kan hij vervolgens ook inzien. Tevens kan hij zien welke organisaties wanneer welke informatie hebben ingezien. Inderdaad, ook is tot de persoon herleidbaar wie die informatie heeft geraadpleegd. Tegen dat gebruik is bezwaar mogelijk. Zo krijg je als burger dus weer voor een deel de regie over je informatie terug. Zichtbaar wordt wanneer particuliere belangen van een persoon of organisatie ten onrechte het algemeen belang overvleugelen. Of wanneer de overheid ten onrechte het algemeen belang inroept om particuliere belangen in te perken.

9. Hoe nu verder?

De netwerksamenleving is onontkoombaar. Voortgaan met het bieden van specifieke oplossingen voor specifieke vragen en problemen leidt niet tot echte oplossingen. Dat is een doodlopende straat. Het roer moet om, op weg naar een stelselmatige aanpak van authenticatie en autorisatie; zie figuur 13 voor een overzichtsschema. We zullen met zijn allen moeten inzetten op oplossingen die voor in principe elke transactie geschikt en bruikbaar zijn. Publiek en privaat, nationaal en internationaal. Door dat te doen bouw je aan een informatie-infrastructuur die voor iedereen toegankelijk is. Door de informatie die voor identity management nodig is centraal te zetten, en niet de techniek, maak je bovendien oplossingen die tijdloos zijn en passen bij de menselijk maat.

Peter Waters (1947) is hoofd van het Bureau Forum Standaardisatie, een onderdeel van Logius. Voorheen heeft hij als beleidsmaker bij de overheid gewerkt (ministerie van Binnenlandse Zaken en Koninkrijksrelaties) en als consultant in het bedrijfsleven, Rode draad in zijn carrière is de vindbaarheid en hergebruik van overheidsinformatie.

¹¹ De Wetenschappelijke Raad voor het Regeringsbeleid (WRR) vraagt in het rapport *iOverheid* (Amsterdam University Press, 2011) onder meer aandacht voor de wenselijkheid te kunnen zien of informatie uit verschillende databases onderling met elkaar zijn vergeleken en/of gekoppeld. Dat vestigt immers een nieuwe context van het gebruik.



Figuur 13:
op weg naar een stelselmatige aanpak
van authenticatie en autorisatie.

