IDENTITEITSMANAGEMENT IN NEDERLAND

DE STAND VAN ZAKEN

ECP NL

EPN

Identiteitsmanagement in Nederland

De stand van zaken

Een productie van:

ECP NL

EPN

Colofon

Dit is een uitgave van ECP-EPN, Platform voor de informatiesamenleving. Deze rapportage is tot stand gekomen dankzij een bijdrage van het ministerie van Economische Zaken.

Teksten:
mr Rachel Marbus

Ontwerp omslag en binnenwerk:
ECP-EPN

Druk:
Efficiënta Offsetdrukkerij bv

ISBN: 9789076957241

Inhoudsopgave

Inleiding

Identiteiten en het beheren daarvan (identiteitsmanagement) winnen steeds meer aan belang in digitaal Nederland. In verschillende sectoren, zoals onder meer de overheid en het bedrijfsleven, wordt hard gewerkt aan het realiseren en vervolgens gebruiken van verschillende systemen om de identiteiten van burgers en klanten te beheren. Er wordt niet alleen ongelofelijk veel werk verzet op het gebied van identiteitsmanagement, maar ook erg veel kennis vergaard. Het werk gebeurt nu nog veelal binnen de eigen 'zuilen', maar toch is er een steeds sterker wordende roep om samen te werken en informatie te delen. Eén manier om daaraan ten dele tegemoet te komen is het in kaart brengen van de stand van zaken op het gebied van identiteitsmanagement in Nederland.

In deze rapportage wordt eerst gekeken naar wat identiteitsmanagement nu precies is; wat verstaan wij daaronder? Daarnaast worden verschillende sectoren doorgelicht en wordt aan de hand van een aantal korte cases een beeld geschetst van wat er allemaal voor handen is en waar we staan. Dit rapport zal niet elk systeem kunnen behandelen, daarvoor is simpelweg niet genoeg tijd en plaats. Toch is geprobeerd om een zo volledig mogelijk overzicht te geven. In het rapport zelf zal daarom bij een aantal systemen nader worden stilgestaan ter illustratie van het geheel. De cases die behandeld worden in dit rapport zijn uitgezocht op grond van het soort systeem waarvan sprake is. Daarbij is gepoogd om zoveel mogelijk diversiteit te behandelen en de verschillende mogelijkheden binnen het identiteitsmanagement aan bod te laten komen.

Tevens gaat dit rapport in op mogelijke knelpunten en vraagstukken die spelen op het gebied van identiteitsmanagement in zijn algemeenheid. Daarbij komen ondermeer vragen aan de orde rondom privacy, identiteitsdiefstal en/of -fraude en medegebruik van identiteitsmanagementsystemen. Ook worden de verschillende belangen van de betrokken partijen in kaart gebracht waarna bekeken wordt hoe de verschillende belangen zich tot elkaar verhouden.

Doelstelling:
Het in kaart brengen van de stand van zaken op het gebied van identiteitsmanagement, waarbij de focus ligt op Nederland.

Vraagstelling:
Wat is de stand van zaken wat betreft identiteitsmanagement in Nederland?

Deelvragen:
Wat is identiteit en wat is identiteitsmanagement?
Wat zijn de vraagstukken en eventuele knelpunten op het gebied van identiteitsmanagement?

1 Wat is identiteitsmanagement?

1.1 Wat is identiteit?

De vraag naar wat identiteit precies is, blijkt lastig te beantwoorden. Wat het antwoord is, hangt vaak af van wie je de vraag stelt. Een wetenschapper komt met een ander antwoord dan 'Jan met de pet' en een bedrijf heeft vaak ook een geheel eigen visie op datgene wat identiteit nu eigenlijk is. Voor de afbakening van dit rapport nemen we de insteek dat het begrip identiteit toegespitst wordt op persoonlijke identiteit, ook wel de identiteit van personen. Groeps-, etnische of corporate-identiteit vallen daarom dan ook buiten de scope van dit document. Waar in dit rapport van 'identiteit' gesproken wordt, wordt dan ook 'persoonlijke identiteit' bedoeld.

1.1.1 Historische setting van persoonlijke identiteit

Dan rest de vraag wat nu eigenlijk persoonlijke identiteit is. Binnen de sociale wetenschappen wordt al jarenlang gediscussieerd over de vraag wat identiteit is en hoe identiteit tot stand komt. Vraagstukken over persoonlijke identiteit maken één ding duidelijk: hoe mensen denken over persoonlijke identiteit verandert met de tijd.[1] Het begrip identiteit is telkens aan verandering onderhevig door ontwikkelingen in de maatschappij en de cultuur.[2] Identiteit wordt vooral gezien als iets dat fluïde is en daardoor dus ook niet als begrip vaststaat.[3] Dit is echter niet altijd zo geweest. Verschillende wetenschappers en geschiedkundigen hebben gedebatteerd over de vraag wanneer en hoe persoonlijke identiteit als onderwerp onder de aandacht werd gebracht. Waar de meeste wetenschappers het wel over eens zijn, is het feit dat er in de Middeleeuwen amper sprake was van identiteit en individualiteit.[4] Dit had verschillende redenen: er bestond een streng systeem van rangen en standen met voorgedefinieerde rollen voor iedereen, er was weinig sociale mobiliteit en ook het strenge christelijke geloof stond individualiteit in de weg.[5]

In de periode die daarop volgt, zien geschiedkundigen dat er steeds meer aandacht komt voor het individu en persoonlijke privacy.[6] De eerste geleerde die zich in het debat over identiteit opwerpt, is Descartes (net voor de tweede helft van de 17e eeuw).[7] Zijn opvattingen over het zelf zijn van grote invloed geweest op het verdere debat rondom persoonlijke identiteit.[8] Volgens Descartes is het zelf een denkend en rationeel wezen. Zijn beroemde adagium "I think, therefore I am" plaatst het zelf in een logische setting. Daarmee introduceert hij een rationele manier om naar de mensheid en identiteit te kijken.[9] In de periode volgend op de Verlichting maakt het denken over identiteit wederom een transformatie door.[10] Gedurende de Romantische periode is er een groeiende interesse in persoonlijkheid en persoonlijke ontwikkeling.[11] De Romantische denkers plaatsen de mens als uniek wezen op de voorgrond; ieder mens is uniek en deze uniciteit is van hoge waarde.[12] Er kwam daarmee een groeiende aandacht voor het individu; in biografieën werden steeds meer persoonlijke feiten verteld en kleding vormde een uiting van persoonlijkheid en was niet langer gebonden aan rangen en standen. Volgens Baumeister betekenen deze veranderingen dat persoonlijkheid belangrijker gevonden werd dan sociale status als onderdeel van de persoonlijke identiteit.[13]

In de jaren die volgen wordt Descartes' manier van denken over de mens scherp bekritiseerd. Vooral de zogenaamde Pragmatische[14] denkers als William James,

1 Baumeister 1986, p. 4.
2 Back 1989, p. 222.
3 Elliot 2001, p. 4. Zie ook: Gergen 1991, p. 16.
4 Anderson 1997, p. 13-14.
5 Anderson 1997, p. 13-14, Baumeister 1986, p. 30.
6 Anderson 1997, p. 14-15.
7 In 1641 schreef hij zijn zeer invloedrijke werk *Meditations on First Philosophy*. Hierin introduceerde hij de zinsnede: "I think, therefore I am".
8 Frissen & De Mul 2000, paragraaf 2, 'Transformatie van het moderne identiteitsbegrip', Holstein & Gubrium 2000, p. 18-21. Zie ook: Baumeister 1986, p. 11-12.
9 Holstein & Gubrium 2000, p. 18.
10 Zie hierover: Baumeister 1986, p. 59-95.
11 Baumeister 1986, p. 59.
12 Baumeister 1986, p. 63. Gergen 1991, p. 27.
13 Baumeister 1986, p. 64-65.
14 Pragmatisch denken komt voort uit de filosofie en kent zijn oorsprong in de Verenigde Staten in de late jaren 1800. Voor een korte introductie over Pragmatisch denken zie: <http://www.wikipedia.org>.

Charles Horton Cooley, en George Herbert Mead stellen dat identiteit niet alleen gezien kan worden als een rationeel gegeven. Wat zij zeggen is dat je het zelf helemaal niet los kan zien van zijn sociale omgeving en specifieke context. Het zelf is niet een op zichzelf en losstaande entiteit. Sociale invloeden vanuit onze omgeving en de invloed van andere mensen zijn van wezenlijk belang bij het vormen van onze identiteit.[15] Hier doet ook het idee zijn intrede dat identiteit meervoudig is; we hebben verschillende relaties met verschillende mensen en daarbij past het dat de identiteit van een persoon binnen die verschillende relaties ook anders is.[16] Het zelf is opgedeeld in verschillende delen: identiteiten. Elk van deze identiteiten is gekoppeld aan een sociale structuur.[17] Deze verschillende identiteiten brengen dan ook mee dat mensen in bepaalde rollen zichzelf anders voordoen dan in andere: *"Many a youth who is demure enough before his parents and teachers, swears and swaggers like a pirate among his 'tough' young friends".*[18] Persoonlijke identiteit wordt gevormd door sociale interactie.[19] De maatschappij en de persoon zijn afhankelijk van elkaar. Mensen maken de samenleving en de samenleving maakt de mens.[20] Het proces van de sociale interactie tussen mensen is verantwoordelijk voor het ontstaan van deze meerdere 'zelven'.[21]

Het Pragmatisch denken over identiteit heeft tot gevolg dat de discussie een andere koers inzet. De maatschappelijke veranderingen in de 20e eeuw zorgen ervoor dat wetenschappers opnieuw gaan nadenken over persoonlijke identiteit.[22] Industrialisatie, technologische ontwikkelingen en economische afhankelijkheid worden gezien als de belangrijke sociale invloeden van de 20e eeuw.[23] Door deze aspecten is er sprake van een steeds belangrijker wordende handel en een daarmee gepaard gaande reclame. Juist die reclames brengen verandering in het beeld van persoonlijke identiteit. Reclame brengt het ideaalbeeld van een wenselijke identiteit teweeg. Reclamemakers leggen steeds vaker een link tussen bepaalde producten en een 'droomidentiteit'.[24] Ook de opkomst van de massamedia brengt veranderingen in de beeldvorming rondom identiteit, doordat mensen in aanraking komen met andere ulturen en andere opvattingen.[25]

Moderne denkers erkennen dat deze veranderingen in de maatschappij hun weerslag hebben op de persoonlijke identiteit. Rond 1980 doet het zogenaamde post-Moderne denken zijn intrede en alweer wordt verder gedacht over veranderingen in het beeld rondom persoonlijke identiteit. Een aantal 'nieuwe' ideeën doet de ronde. Zo wordt het zelf gepositioneerd als gefragmenteerd. Er zou geen consistentie bestaan in datgene wat het zelf tot het zelf maakt. Dit wordt toegeschreven aan het bestaan en de ontwikkeling van nieuwe technologieën.[26] Daarnaast stellen post-Moderne denkers dat de mens steeds egocentrischer wordt; uiterlijk en voorkomen worden steeds belangrijker.[27]

Moderne denkers zien steeds meer vrijheid voor de mens wat betreft de vorming van zijn identiteit. Zo stelt Giddens bijvoorbeeld dat het zelf een zogenaamd reflexief project wordt.[28] De vorming van persoonlijke identiteit wordt een 'onderneming' an sich.[29] Binnen ons levensverhaal hebben we steeds meer keuzes die we kunnen maken waarmee we onze persoonlijke identiteit vormgeven.[30] Ook de invloed van nieuwe technologie op de vorming van persoonlijke identiteit wordt opnieuw onder de aandacht gebracht. Volgens Gergen zorgen deze nieuwe technologische ontwikkelingen ervoor dat het mogelijk is dat we met steeds meer mensen

15 Elliot 2001, p. 5-6.
16 James 1890, p. 295, Holstein & Gubrium 2000, p. 24.
17 Leary & Price Tagney 2003, p. 132.
18 James 1890, p. 295.
19 Cooley 1922, p. 36.
20 Cooley 1922, p. 42.
21 Mead 1934, p. 142. Holstein & Gubrium 2000, p. 24.
22 Gergen 1991, p. 18-47.
23 Baumeister 1986, p. 77 en p.80.
24 Baumeister 1986, p. 81.
25 Baumeister 1986, p. 82.
26 Elliot 2001, p. 136.
27 Elliot 2001, p. 136.
28 Giddens 1991, p. 19. Giddens 1991, p. 3.
29 Giddens 1991, p. 53.
30 Giddens 1991, p. 5.

steeds meer relaties kunnen aangaan. De hoeveelheid aan verschillende relaties en de hoeveelheid in soorten van relaties neemt hand over hand toe.[31] De hoeveelheid identiteiten daarmee ook. Het gevolg daarvan is dat persoonlijke identiteit steeds meer een maakbaar iets wordt dat telkens aan verandering onderhevig is.[32]

1.1.2 Constanten in identiteitsbegrip & online invloeden

Als we kijken naar het begrip persoonlijke identiteit dan zijn daar een aantal aspecten aan verbonden. Het begrip persoonlijke identiteit is:

Flexibel en veranderlijk: hoe over identiteit gedacht wordt is afhankelijk van onder meer de tijd waarin we ons bevinden, de maatschappij en de normen en waarden die daar heersen en de cultuur.

Meervoudig: hoewel verschillende auteurs erkennen dat er zoiets bestaat als een kernidentiteit (het ik, het ego), wordt algemeen erkend dat een identiteit meervoudig is. Elke persoon heeft meerdere deelidentiteiten, meerdere rollen die in verschillende contexten in het leven tot uiting komen.

Ook wat betreft online identiteiten komen deze constanten voor. Wellicht komen de aspecten flexibiliteit en veranderlijkheid daar nog duidelijker tot uiting. Online is het immers nog veel makkelijker om verschillende identiteiten aan te nemen en/of aan te passen dan dat offline het geval is. Het 'aanmeten' van een andere identiteit kan in de offline wereld nog weleens tot lastige vragen leiden (want waarom doe je je nu ineens anders voor?), in de online wereld lijkt het veel gemakkelijker om iemand anders te worden. Daarbij moet echter wel de kanttekening gemaakt worden dat ook online een eenmaal langer bestaande identiteit met de daarmee gepaard gaande reputatie en kring van mensen daaromheen, een zekere bestendigheid krijgt. Ja, veranderingen zijn altijd mogelijk, maar een radicale omzwaai zal wellicht door de digitale vriendenkring ook moeilijker begrepen worden. Ook het aan identiteit verbonden aspect van meervoudigheid komt in de online wereld duidelijk naar voren. We zijn klant bij verschillende online winkels, zijn actief op sociale netwerksites, hebben online contact met onze overheid en nog vele zaken meer. Al deze verschillende rollen moeten uit elkaar gehouden worden. Hierdoor neemt het belang van goed identiteitsmanagement steeds meer toe.

1.1.3 Waarom is identiteit online anders?

Is er nu een duidelijk verschil tussen het begrip offline identiteit en online identiteit? Het meest voor de hand liggende verschil is uiteraard het feit dat online identiteit gedigitaliseerd is. En dit brengt een aantal zaken mee wat betreft het identiteitsconcept. Zo is in de online wereld in principe veel aan elkaar te linken. Verschillende identiteiten komen daardoor steeds vaker en makkelijker met elkaar in contact. Dit in tegenstelling tot de offline wereld waar onze verschillende deelidentiteiten ook wel met elkaar in contact kunnen komen, maar dit vaak wat lastiger gerealiseerd wordt dan in de online wereld. Ook het persistent zijn van identiteitsinformatie maakt dat er van verschillen gesproken kan worden. Onbedoeld geven mensen online vaak veel van zichzelf prijs (of anderen doen dat voor hen) en jaren later kan deze informatie weer met een paar muisklikken teruggevonden worden.

Vaak wordt, als men het heeft over online identiteit (ook wel virtuele identiteit), eerder een technisch-pragmatisch standpunt aangenomen om te definiëren wat onder 'identiteit' verstaan wordt. Een identiteit in een online omgeving moet vaak – wat betreft het identiteitsmanagement – teruggebracht worden tot 'attributen'. Een attribuut kan bijvoorbeeld de kleur van iemands ogen zijn, zijn naam, adresgegevens en vele zaken meer. Tezamen genomen vormen attributen iemands online identiteit. Welke attributen daarvoor noodzakelijk zijn, is afhankelijk van de betreffende situatie. Het is echter niet correct om te stellen dat een pakketje attributen tezamen genomen iemands (deel)identiteit vormt. Om in een online wereld identiteiten te kunnen managen moet een aanbieder echter vaak wel gebruik maken van deze 'identiteitsreductie'. Juist door deze andere benadering van het begrip identiteit kunnen botsingen ontstaan wat betreft de sociale en bredere aspecten die aan het identiteitsbegrip verbonden zijn. Ook kan het hanteren van

31 Gergen 1991, p. 3 en 32.
32 Gergen 1991, p. 7.

bepaalde technische middelen voor het beheren van identiteit allerlei neveneffecten met zich brengen die een beperkende werking hebben op identiteit. Over deze zaken wordt gesproken in hoofdstuk 5 waar de verschillende vraagstukken op het gebied van identiteitsmanagement aan bod komen.

1.2 Wat is identiteitsmanagement?

Het eenduidig definiëren van identiteitsmanagement is vrij lastig. Verschillende auteurs hanteren verschillende definities en om identiteitsmanagement samen te vatten als 'het beheren van identiteiten' zou het vaak veelomvattende proces geen recht doen. Vaak wordt als uitgangspunt een technische benadering genomen. Zo definiëren Valkenburg en Jurg identiteitsmanagement als: "[identiteitsmanagement] bestaat uit processen en alle onderliggende techniek voor het aanmaken, beheer en gebruik van elektronische identiteitsgegevens".[33] Dit is een vrij pragmatische benadering van identiteitsmanagement. Vaak verschillen de definities al naar gelang de zienswijze die achter de verschillende benaderingen van identiteitsmanagement schuil gaan. Over deze verschillende wijzen van het beheren van identiteiten, komen we nog te spreken in de navolgende paragrafen. Een andere benadering geeft dus vaak een andere definitie. Zo is te zien aan de definitie die binnen het PRIME project gehanteerd wordt. Binnen PRIME wordt identiteitsmanagement gedefinieerd als: "Identity management means managing various partial identities (usually denoted by pseudonyms) of an individual person, i.e., administration of identity attributes including the development and choice of the partial identity and pseudonym to be (re-)used in a specific context or role".[34] Hier gaat het dus om het beheren van de verschillende deelidentiteiten van een persoon met daarnaast een mechanisme voor de gebruiker om te kunnen kiezen uit verschillende deelidentiteiten. Ook wordt rekening gehouden met zogenaamde pseudoniemen (een soort alias) waarmee iemand een bepaalde online handeling kan verrichten. En mocht de gebruiker dit willen, dan kan dit pseudoniem, dat gebruikt werd binnen een bepaalde context, ook weer hergebruikt worden. Zo kan bijvoorbeeld een reputatie opgebouwd worden waarmee het vertrouwen in de online communicatie toeneemt (of afneemt als de reputatie slecht is). Een dergelijke definitie omvat dus veel meer dan de technisch-pragmatische definitie van Valkenburg en Jurg. Maar voordat we overgaan naar het behandelen van de verschillende manieren waarop identiteit beheerd wordt, moeten we eerst stilstaan bij de basisvraag wat er nu precies gebeurt met een identiteit als daarvan gebruik gemaakt gaat worden.

1.3 Het technische procesverloop: Identificatie, Authenticatie en Autorisatie

Als gesproken wordt over identiteitsmanagement, komen vaak als eerste vrij technische overwegingen aan de orde. Hoe verloopt het proces nu precies? Welke stappen worden er in technische zin gezet voordat iemand aan de slag kan met zijn identiteit en wat komt daar nu bij kijken? Deze paragraaf zal daarom kort ingaan op de eerste stappen die gezet worden om een identiteit in online omgevingen te managen. Doorgaans wordt dit technische proces in een aantal elkaar opvolgende stappen omschreven. Nadat iemand is geïdentificeerd, vindt vervolgens authenticatie van die identiteit plaats, een laatste mogelijke stap is dan autorisatie van de desbetreffende identiteit.

Nadat een identiteit is aangemaakt door een persoon, kan deze gebruikt gaan worden. Door middel van verificatie wordt de aan het systeem gepresenteerde identiteit gematched als zijnde een identiteit die bij het systeem bekend is. De identificatie vindt daarmee plaats. Het verifiëren van de identiteit verwijst naar de mechanismen voor het aanmaken van een identiteit waarmee in een later stadium bepaalde claims kunnen worden gedaan met betrekking tot die desbetreffende identiteit (ik ben wie ik zeg dat ik ben).[35]

"Met authenticatie wordt het proces bedoeld waarmee een persoon zijn of haar identiteit kan aantonen, dat wil zeggen: kan zeggen dat hij of zij inderdaad is wie hij of zij zegt te zijn".[36] Bij authenticatie gaat het er dus om

33 Valkenburg en Jurg 2007, p. 36.
34 A. Pfitzmann, M. Hansen, Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology, Version v0.31 February 15, 2008.
35 Srivastava et al 2006, p. 114.
36 Valkenburg en Jurg 2007, p. 38.

dat aangetoond kan worden dat een persoon ook daadwerkelijk is wie hij zegt dat hij is.[37] Authenticatie wordt gedaan met gebruik van bepaalde middelen. Daarbij valt te denken aan de combinatie van een gebruikersnaam met een wachtwoord, maar ook aan een smartcard of een biometrisch middel als een vingerafdruk. Binnen authenticatiemiddelen maakt men vaak onderscheid tussen sterke en zwakke middelen. Dit onderscheid wordt gemaakt op grond van de relatieve mate van zekerheid die door middel van het gebruikte authenticatiemiddel kan worden verkregen over de identiteit van een persoon. Sterke vormen van authenticatie bestaan uit iets dat de gebruiker weet (een pincode) en iets dat de gebruiker heeft (een 'token' of een biometrisch middel). Dan is dus sprake van een cumulatie van middelen. Zwakke middelen bestaan vaak uit slechts één middel zoals een wachtwoord met usernaam combinatie.[38] Bij authenticatie gaat het er overigens niet om dat de offline identiteit van een persoon bekend is. In het proces van authenticatie gaat het er slechts om toegang te verlenen tot een bepaalde dienst. Wie achter de identiteit schuil gaat, is daarbij niet van belang.[39]

"Autorisatie is het proces van het verlenen van toegang aan personen of systemen tot (delen van) de functionaliteit van ICT-diensten".[40] Bij het proces van autorisatie gaat het erom degene die geïdentificeerd is een bepaalde rol toe te bedelen. Behoort iemand tot een bepaalde groep, mag hij of zij bepaalde informatie zien, is hij of zij gerechtigd bepaalde handelingen te verrichten etcetera?[41] Autorisatie gebeurt daarmee op basis van rollen. Aan die rollen zijn bepaalde bevoegdheden gekoppeld. Zo zal een systeembeheerder vaak meer mogen dan bijvoorbeeld een werknemer. Die rollen zijn dus gekoppeld aan iemands identiteit. Daarnaast wordt ook vaak onderscheid gemaakt met betrekking tot de omstandigheden waarin iemand verkeert. Op kantoor kan iemand bijvoorbeeld toegang hebben tot alle faciliteiten van het bedrijf waar hij werkt, maar indien diezelfde persoon vanaf huis toegang tot het netwerk wil verkrijgen, kan bepaald worden dat specifieke informatie niet toegankelijk is. Dit wordt ook wel 'policy based access' genoemd.[42] Aan de basis hiervan ligt de zogenaamde 'role based access control'; hierin worden een bepaalde hoeveelheid rollen gedefinieerd. Aan deze rollen worden toegangsrechten gekoppeld en aan de rollen worden vervolgens gebruikers gekoppeld.[43]

De hier besproken onderdelen wat betreft het managen van identiteit zijn vrij fundamentele zaken die in principe voor alle processen van identiteitsmanagement gelden. Maar hoe er nu daadwerkelijk met de identiteiten van gebruikers wordt omgegaan in concrete gevallen is daarmee nog niet duidelijk. Het managen van identiteiten kent namelijk een aantal verschillende verschijningsvormen die elk vanuit een verschillende benadering worden vormgegeven. In het hiernavolgende hoofdstuk wordt daarom stilgestaan bij de verschillende zienswijzen op identiteitsmanagement. Hierbij worden de voordelen en de nadelen van de behandelde systemen steeds besproken.

37 Valkenburg en Jurg 2007, p. 38.
38 Valkenburg en Jurg 2007, p. 38.
39 Van Kokswijk 2007, p. 171.
40 Valkenburg en Jurg 2007, p. 39.
41 Valkenburg en Jurg 2007, p. 16.
42 Valkenburg en Jurg 2007, p. 19.
43 Valkenburg en Jurg 2007, p. 39.

2. Identiteitsmanagement in verschillende verschijningsvormen

In dit hoofdstuk komen verschillende vormen van identiteitsmanagement aan de orde. Het gaat daarbij ook vaak om bepaalde zienswijzen over hoe een ideaaltype identiteitsmanagement er uit zou moeten zien. De verschillende vormen en zienswijzen worden hier zo volledig mogelijk omschreven. Daarbij moet in ogenschouw worden genomen dat deze behandeling van verschillende zienswijzen niet tot bedoeling heeft aan te geven dat één bepaalde zienswijze of vorm van identiteitsmanagement de beste is. Een bepaald systeem kan zeer goed werken in een bepaalde context maar binnen een andere context juist niet goed passen. Zo zal een systeem rondom het doen van online betalingen bijvoorbeeld meer veiligheidswaarborgen moeten bevatten dan een systeem dat mensen toegang geeft tot een website waar de gebruiker commentaar op bijvoorbeeld het nieuws kan plaatsen. Zo heeft elk systeem zowel voordelen als nadelen in het gebruik. En, ook spelen er verschillende belangen bij de keuzes voor een bepaald systeem. De verschillende belangen rondom identiteitsmanagement komen later nog apart aan de orde in hoofdstuk 4.

2.1 Ontwikkelingen binnen identiteitsmanagement

Alvorens meer specifiek in te gaan op deze verschillende systemen moet eerst een korte introductie worden gegeven over wat precies beoogd wordt met de verschillende te behandelen systemen. Bepaalde wijzen van identiteitsmanagement roepen namelijk vragen op en in de ontwikkeling van nieuwe zienswijzen (als reactie op mogelijke tekortkomingen in reeds bestaande systemen) wordt telkens geprobeerd om aan die vragen tegemoet te komen. Met de beschrijving van zowel de ontwikkeling van de verschillende systemen als de concrete werking ervan, wordt beoogd inzicht te verschaffen in de mogelijkheden en onmogelijkheden van het managen van identiteiten in een online wereld.

De eerste ontwikkelingen rondom identiteitsmanagementsystemen waren zeer bedrijfsgedreven. De noodzaak tot het ontwikkelen van een systeem om identiteiten te beheren werd namelijk door hen als een van de eersten gevoeld. Zij ontwikkelden systemen om de gegevens van hun klanten/gebruikers te beheren. Het zogenaamde 'enterprise centric' of ook wel silo/site identiteitsmanagement wordt door bedrijven ingezet om maximaal aan hun behoeften tegemoet te komen. Voor bedrijven is het daarbij zaak om klanten te kunnen identificeren en authenticeren. Gegevens van klanten/gebruikers worden daarbij op een centrale plek opgeslagen. Nadelen van een dergelijke benaderwijze zijn dat gebruikers vaak gewongen worden om op een bepaalde manier vorm te geven aan hun identiteit (denk aan het verplicht gebruiken van bijvoorbeeld een e-mailadres als gebruikersnaam). Daardoor kunnen zij gedwongen worden een identiteit aan te maken die ze eigenlijk helemaal niet willen gebruiken. Daarnaast is het niet mogelijk voor gebruikers om hun ene identiteit te gebruiken in verschillende omgevingen binnen hetzelfde bedrijf. Zo kan het voorkomen dat iemand meerdere identiteiten moet bezitten om van de verschillende diensten van slechts één bedrijf gebruik te maken.[44] Een ontwikkeling die daar als reactie op volgde was het zogenaamde 'single organisation single sign on' (SOSSO). Er is in dat geval nog steeds maar sprake van één bedrijf, maar voor alle verschillende diensten/applicaties en toepassingen binnen dat bedrijf kan van dezelfde identiteit gebruik gemaakt worden. Voordelen zijn uiteraard dat de gebruiker minder identiteiten hoeft te onthouden en bijhouden. Het nadeel van een dergelijk systeem is dat het voor gebruikers in principe niet mogelijk is om binnen die ene organisatie meerdere identiteiten te gebruiken. Hierdoor kan een vollediger beeld van iemands handelingen binnen een domein ontstaan en kan geen onderscheid gemaakt worden tussen de verschillende contexten en bijbehorende deelrollen van personen, hetgeen kan leiden tot een samenvallen of versmelten van verschillende contexten.[45]

Met SOSSO wordt de opmaat gegeven voor het zogenaamde federatieve identiteitsmanagement. Bij federatief identiteitsmanagement probeert men de grootte van de 'sleutelbos' voor gebruikers te verkleinen. Tussen verschillende organisaties kan in deze geval-

44 Zie hierover: Ardagna et al 2008, paragraaf 3.4.
45 Zie hierover: Ardagna et al 2008, paragraaf 3.4.

len van eenzelfde identiteit gebruik gemaakt worden voor toegang tot diensten of netwerken. Ook voor de aanbieders/organisaties levert dit meer gebruiksgemak en daarnaast kostenbesparing op. Maar, ook binnen deze vorm van identiteitsmanagement wordt nog niet tegemoetgekomen aan de behoefte van gebruikers om meerdere deelidentiteiten te gebruiken voor verschillende contexten. Daarom is de laatste jaren veel gewerkt aan identiteitsmanagementsystemen waarbij de gebruiker meer centraal komt te staan – het zogenaamde 'user centric identity management'. Binnen dit soort systemen beheren gebruikers zelf hun gegevens, of hebben er in ieder geval meer controle over. Daarmee heeft een gebruiker meer controle over zijn presentatie van het zelf.[46] Vanuit de gedachte dat de gebruiker meer centraal gesteld moet worden in het identiteitsmanagement, is een laatste stroming ontstaan waarin men nog weer een stapje verder gaat. Het gaat daarbij om systemen die de behoefte aan privacy vooropzetten. In deze 'privacy enhancing' systemen staat privacy, het gebruik van meerdere anonieme of pseudonieme deelidentiteiten die niet linkbaar aan elkaar zijn, centraal. De werking van de hier kort aangehaalde systemen komen in de volgende paragrafen aan bod. Deze systemen bestaan naast elkaar, maar er is wel een duidelijke verschuiving in de manier van denken over identiteitsmanagement zichtbaar. Deze verschuiving wordt in paragraaf 3.7 zichtbaar gemaakt door middel van enkele trends op het gebied van identiteitsmanagement.

2.2 Silo of site idm

Bij silo of site gecentreerd identiteitsmanagement gaat het om identiteitsmanagement in een specifieke verschijningsvorm. Deze manier van het beheren van identiteiten van gebruikers wordt ook wel aangeduid als 'enterprise centric'. De gegevens van personen wiens identiteit wordt beheerd worden op één plek opgeslagen en bewaard – daar is ook de term 'silo' van afgeleid.[47] De gebruiker die gebruik wil maken van een bepaalde dienst meldt zich aan bij de betreffende aanbieder. De aanbieder beheert de gegevens van de gebruiker. Dit is een vrij eenvoudige vorm van identiteitsmanagement waarbij in principe niet meer dan twee partijen betrokken zijn. Het gaat dus om systemen die afgesloten zijn van de 'buitenwereld' – zogenaamde 'walled gardens'.[48] Dit systeem kan niet buiten de virtuele muren van de specifieke omgeving c.q. applicatie gebruikt worden. Voordelen van dit systeem zijn dat het voor de dienstenaanbieder vrij eenvoudig te gebruiken is. Daarnaast heeft (afgezien van ongewenste inbreuken op het systeem) in principe alleen de dienstaanbieder toegang tot de persoonlijke gegevens van de gebruikers. Gebruikers hebben niet altijd de vrijheid om zelf een wachtwoord te kiezen waardoor de kans op het vergeten van wachtwoorden toeneemt. En als de gebruikers wel de keuze hebben om zelf een wachtwoord te kiezen, bestaat het risico dat zij juist vanwege het feit dat ze zoveel deelidentiteiten moeten aanmaken, overal hetzelfde wachtwoord gebruiken (of zeer op elkaar lijkende wachtwoorden).

2.3 Federatief idm

Federatief identiteitsmanagement is een verzamelterm voor alle processen, standaarden en technologie die het mogelijk maken om op een gecontroleerde manier identiteitsgegevens uit te wisselen over organisatiegrenzen heen.[49] De gegevens van gebruikers worden door een bepaalde aanbieder opgeslagen en beheerd. De gebruiker kan daarmee gebruikmaken van de diensten van deze specifieke aanbieder. Echter, de authenticatiemiddelen kunnen gedeeld worden zodat een gebruiker ook bij een andere – aangesloten of gelieerde – dienst zich aan kan melden. Een voorbeeld daarvan is het zogenaamde Surfspot waar medewerkers en studenten van bepaalde universiteiten en hogescholen gebruik van kunnen maken om software te bestellen.[50] Inloggen gebeurt met de gebruikersnaam en het wachtwoord van de universiteit of de hogeschool waarbij de medewerker of student aangesloten is. De universiteit of hogeschool controleert of deze persoon daadwerkelijk werkt bij of studeert aan de

46 Zie hierover: Ardagna et al 2008, paragraaf 3.4.
47 Deze vorm van identiteitsmanagement wordt overigens ook wel 'domain centric' identiteitsmanagement genoemd (de gevens worden binnen een bepaald domein gebruikt en opgeslagen/beheerd).
48 Zie hierover ook Dick Hardt in zijn beruchte speech 'Identity 2.0'. De speech is te zien via: <http://identity20.com/media/OSCON2005/>.
49 Valkenburg en Jurg 2007, p. 45.
50 <http://www.surfspot.nl>

desbetreffende school of universiteit. Het resultaat van deze controle wordt doorgegeven aan Surfspot. Daarmee worden dus de bestaande middelen van de universiteit of hogeschool waarbij de gebruiker is aangesloten, gebruikt.

Een dergelijk federatief systeem werkt dus met een 'single sign on'. Daarmee is meteen een van de grote voordelen van een federatief systeem gegeven: het gebruiksgemak. Ook voor de aanbieder van de diensten bestaat gebruiksgemak. Die hoeft niet zelf een systeem te beheren wat betreft het aanmaken van identiteiten van gebruikers doordat zij gebruik kunnen maken van de faciliteiten van de bronaanbieder. Een nadeel van federatieve systemen is de juridische en technische complexiteit.[51] Aanbieders van diensten die zich in de federatie bevinden moeten over een grote mate van wederzijds vertrouwen beschikken dat bijvoorbeeld bepaalde veiligheidsstandaarden daadwerkelijk goed en adequaat zijn in het gebruik. Een systeem als dit is daardoor niet voor elke situatie inzetbaar. Voor de privacy van de gebruiker kan een federatief systeem zowel voordelen als nadelen hebben. Technisch gezien is het mogelijk voor de verschillende aanbieders in een federatief systeem om de persoonlijke informatie van een bepaalde gebruiker te achterhalen. In principe hoeft echter alleen de bronaanbieder toegang te hebben tot de persoonlijke gegevens van een gebruiker. Als een gebruiker toegang wil krijgen tot de diensten van gelieerde aanbieders, kan dit op een anonieme of pseudonieme basis tot stand gebracht worden.[52]

Een voorbeeld van een federatief systeem is OpenID.[53] OpenID werkt net weer even volgens andere principes dan Surfspot, omdat het een gedecentraliseerd systeem is met een single sign on. OpenID werkt met meerdere onafhankelijk van elkaar bestaande providers, vandaar het genoemde decentrale karakter. Elke provider moet zich houden aan een minimum set van standaarden. Door bij zijn eigen OpenID-provider in te loggen, is een gebruiker tegelijkertijd ingelogd bij de aangesloten diensten. Het gedecentraliseerde karakter van OpenID heeft als voordeel dat het systeem blijft functioneren ook als een bepaalde provider zijn dienstverlening staakt. De OpenID van een gebruiker kan namelijk meegenomen worden naar een andere provider. Een dergelijk systeem is minder geschikt voor diensten waarvoor een sterkere vorm van authenticatie mogelijk is, omdat het werkt met alleen een gebruikersnaam en wachtwoord combinatie. Een ander nadeel van een dergelijk systeem is dat gebruikers voor alle gelieerde diensten eenzelfde identiteit gebruiken. Indien iemand liever verschillende identiteiten voor verschillende diensten gebruikt, zou hij meerdere OpenID-accounts moeten aanmaken. Het voordeel van de single sign on is daarmee echter verdwenen.

2.4 User centric idm

Tijdens de bespreking van de hiervoorgaande manier om identiteiten te beheren werd al duidelijk dat er voor de gebruikers weinig plaats is in het geheel. De afgelopen jaren is het blikveld van bedrijfscentraal naar gebruikerscentraal verschoven.[54] De achterliggende gedachte bij een dergelijke visie vindt haar oorsprong in sociologisch gedachtegoed over persoonlijke identiteit en het beheer daarvan in het dagelijks leven. Daarbij wordt het gedachtegoed van Goffman aangehaald om uitleg te geven over de noodzaak van het meer centraal plaatsen van de gebruiker.[55] Het kunnen gebruiken van meerdere deelidentiteiten die elk een specifieke rol van een persoon vertegenwoordigen wordt noodzakelijk geacht voor de sociale ontwikkeling en uiting van het zelf binnen een meervoud van contexten. Bij deze ontwikkeling hoort tevens de noodzaak om over de mogelijkheid te beschikken om de verschillende publieken waarvoor wij deze rollen spelen, te scheiden. Dit komt overigens niet alleen het individu ten goede, maar ook de maatschappij. De mogelijkheid om verschillende rollen en publieken van elkaar te scheiden maakt het onderhouden van relaties, samenwerken in teams, kameraadschap en diversiteit mogelijk.[56] Daarnaast wordt ook het belang onderstreept van het kunnen beheren van de reputatie, het kunnen handelen als een

51 Jøsang et al 2007, paragraaf 4.5.
52 Jøsang et al 2007, paragraaf 4.5.
53 <http://www.openid.net>, <http://www.mijnopenid.nl>
54 Ardagna et al 2008, paragraaf 3.4.
55 Zie hierover Argagna et al 2008, paragraaf 3.3.
56 Ardagana et al 2008, paragraaf 3.3.

autonoom persoon en de noodzaak om inzicht te verkrijgen in hoe anderen het individu binnen een bepaalde context beoordelen. Door bij het managen te denken vanuit de gebruiker en zijn (sociale) behoeften kan aan deze zaken tegemoet worden gekomen.

Bij user centric identiteitsmanagement is de gebruiker de bepalende factor, waarnaast nog steeds oog is voor de belangen van de aanbieder van de dienst. Hierbij wordt de controle over de persoonlijke gegevens en de persoonlijke identiteit weer teruggelegd bij de gebruiker. Verzoeken om informatie over de gebruiker worden namelijk eerst aan de hem voorgelegd. Nadat die zijn goedgekeurd, kan de datatransactie plaatsvinden.[57] Overigens hoeft een gebruiker niet altijd letterlijk zelf op de 'ok-knop' te klikken, hij kan daarvoor ook een agent inzetten die gebaseerd op vooraf ingestelde regels de transactie kan goed-, of afkeuren.[58] Het gebruik van de persoonlijke gegevens van de gebruiker wordt zichtbaar en daarmee wordt een grotere controle over deze gegevens voor die gebruiker mogelijk.[59] Dataminimisatie is daarbij het sleutelwoord.[60] Dit laatste ligt zeer dicht aan tegen de privacyverhogende visie op identiteitsmanagement.

2.5 Privacy enhancing idm

In een systeem dat gebaseerd is op de gedachte van 'privacy enhancing identity management' (privacyverhogend identiteitsmanagement) staat niet alleen de gebruiker centraal, maar vooral ook de privacy wat betreft de persoonlijke gegevens en de privé sfeer van de gebruiker. In dergelijke privacyverhogende systemen gaat het erom dat een gebruiker zelf controle heeft over zijn digitale identiteit en zijn verschillende deelidentiteiten in een online wereld.[61] Dit is het basisuitgangsprincipe zoals dat hierboven in de user centric manier van identiteitsmanagement werd weergegeven. De zaken die daar besproken werden, gelden dan ook onverkort voor de privacyverhogende systemen die hier aan de orde zijn.

Volgens Hansen et al moet een privacyverhogend systeem aan een aantal vereisten voldoen. Er moet sprake zijn van een veilige infrastructuur die pseudonimiteit toestaat. Daarbij moet tevens aandacht zijn voor vertrouwelijkheid, integriteit en authenticiteit. Binnen het systeem moet het mogelijk zijn om desgewenst anoniem te kunnen communiceren.[62] Uiteindelijk gaat het er binnen deze systemen om dat de gebruiker kiest welke mate van pseudonimiteit hij in een bepaalde situatie wenst te gebruiken. Daarbij moet het nog steeds mogelijk zijn om over de gebruikelijke opties te kunnen beschikken wat betreft identificatie, authenticatie en authorisatie.[63] Een systeem wordt geacht privacyverhogend te zijn als het in afdoende mate verzekert dat de verschillende deelidentiteiten van een persoon niet aan elkaar gekoppeld kunnen worden.[64] Dit betekent dat een buitenstaander – denk bijvoorbeeld aan een hacker – twee verschillende delen van iemands identiteit niet aan elkaar kan plakken.[65] Om dit te realiseren, werkt een privacyverhogend systeem met pseudoniemen. Een pseudoniem, samen met de data die daaraan gelinkt zijn, vormt een deelidentiteit.

Een privacyverhogend systeem werkt met zogenaamde cryptografische *credentials*. Een *credential* is bijvoorbeeld het gegeven dat een persoon ouder is dan 18 jaar. Maar een *credential* kan ook heel goed een gegeven als iemands adres bevatten. Een *credential* waarmee bijvoorbeeld aangegeven wordt dat iemand ouder is dan 18 jaar kan aan een bepaalde pseudonieme identiteit worden gekoppeld.[66] In bepaalde situaties volstaat dit. Meer gegevens van een persoon hoeven niet nodig te zijn.[67] Denk bijvoorbeeld aan de

57 P.J. Windley, 'User-centric identity brings federation close to home. Agreements between peers can add up to an effective federation', Infoworld, 24 maart 2006.
58 Dhamija & Dusseault 2008, p. 26.
59 Hansen et al 2004, p. 36.
60 Hansen er al 2004, p. 36.
61 Hansen et al 2004, p. 35.
62 Hansen et al 2004, p. 36.
63 Hansen et al 2004, p. 38.
64 A. Pfitzmann, M. Hansen, Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology, Version v0.31 February 15, 2008, p. 31.
65 A. Pfitzmann, M. Hansen, Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology, Version v0.31 February 15, 2008, p. 12.
66 Hansen et al 2004, p. 37.
67 Hansen et al 2004, p. 38.

toegang tot pornografische websites. Het kunnen vaststellen dat iemand oud genoeg is om de content te bekijken, is voldoende.[68] In deze situatie is echter wel een derde, onafhankelijke partij nodig die de gegevens op een dergelijk credential certificeert (om erop te kunnen vertrouwen dat de gegevens juist zijn).[69] De credentials die in een privacyverhogend systeem gebruikt worden, worden door middel van crypotografie omgezet in alleen voor de computer leesbare code. Dit voorkomt dat eventuele persoonlijke gegevens door (niet geautoriseerde) derden gelezen kunnen worden. In gevallen van fraude of als er een geschil is gerezen kan de identiteit van de persoon die schuilgaat achter de credentials en de pseudonieme identiteit vervolgens onthuld worden door de derde partij in het geding; de verlener van de credentials.[70] Een dienstaanbieder heeft daardoor altijd de mogelijkheid om de gebruiker – om welke reden dan ook – aansprakelijk te stellen voor bepaalde daden.[71]

2.6 Afsluiting

De hierboven besproken vormen van identiteitsmanagement komen allemaal voor in de praktijk. Echter, niet altijd in de specifieke vorm zoals besproken. Verschillende zienswijzen en systemen worden gecombineerd of door elkaar gebruikt al naar gelang de situatie. Zo kan een identiteitsmanagementsysteem gebaseerd zijn op een user centric gedachte, maar in de vorm van een silo gegoten zijn. Ook kan een user centric systeem in een federatieve vorm gegoten worden.[72] Jøsang et al geven een voorbeeld van hoe een dergelijk user centric silosysteem er uit kan zien. In deze situatie kan een gebruiker inloggen door zijn mobiele telefoon te gebruiken. Als een gebruiker toegang wil krijgen tot een dienst, kan hij een eenmalige inlogcode toegestuurd krijgen via een sms. Die code werkt als een sleutel waarmee de deur naar de dienst geopend wordt. De dienst beschikt over de gegevens van de gebruiker en heeft deze in beheer. De gegevens worden niet gedeeld met andere aanbieders. Als meerdere aanbieders gebruikmaken van deze optie tot inloggen door middel van codes die toegestuurd worden via sms, ontstaan er verschillende zogenaamde silo's naast elkaar.[73] Groot voordeel van deze situatie is dat de gebruiker niet een veelvoud aan identiteiten en gekoppelde wachtwoorden hoeft te onthouden. Uiteraard zal een gebruiker zichzelf in ieder geval eenmaal moeten inschrijven bij de verschillende aanbieders van de diensten.

68 Dit kan anders zijn in die gevallen dat er sprake is van betaalde content achter de 'voordeur'. Om voor de toegang tot die content te kunnen betalen, zal meer informatie nodig zijn.
69 Camenisch et al 2005, paragraaf 3.2.
70 Camenisch et al 2005, paragraaf 2.
71 Camenisch et al 2005, paragraaf 5, Hansen et al 2004, p. 37.
72 Zie hierover bijvoorbeeld: Jøsang et al 2007, paragraaf 5.2.
73 Jøsang et al 2007, paragraaf 5.2.

3 Sectoren in Nederland

In dit hoofdstuk worden verschillende voorbeelden gegeven van systemen waarbinnen met identiteiten wordt omgegaan. Diverse sectoren komen aan bod waarbinnen een aantal korte cases behandeld wordt ter illustratie van de diverse systemen die binnen Nederland gebruikt worden voor het omgaan met en het beheer van identiteiten.

3.1 Welke sectoren worden behandeld en waarom?

Op verschillende plekken in Nederland wordt op verschillende manieren omgegaan met het beheren van identiteiten. Elke sector heeft zo zijn eigen wensen en eisen. In dit hoofdstuk lichten wij een aantal sectoren aan de hand van cases nader uit. Per sector wordt ten minste één specifiek voorbeeld van een identiteitsmanagementsysteem of van het beheer van identiteiten binnen een specifieke context gegeven. Daarbij is besloten om zo breed mogelijk in te zetten en verschillende relaties en soorten systemen aan bod te laten komen. Zo is er plaats voor de verhouding burger/bedrijf – overheid, zorgverlener – patiënt, onderwijsinstelling – student/medewerker, bedrijf – consument en personen onderling in sociale setting. Daarnaast wordt gekeken naar federatieve systemen, meer open en meer gesloten systemen en systemen waarbinnen de gebruiker zelf zijn identiteitsbeheer in de hand heeft. Tevens wordt aandacht besteed aan het onderscheid tussen systemen die gebruikmaken van zogenaamde 'lichte' authenticatiemiddelen en systemen die – vanwege zwaarderwegende achterliggende belangen – gebruikmaken van 'sterke' authenticatiemiddelen.

3.2 De overheid

Bij de overheid gaat het om communicatie tussen de overheid en burgers of tussen de overheid en het bedrijfsleven. Digitale communicatie met de overheid en het authenticeren van de identiteit van ofwel de burger ofwel het bedrijf gebeurt door middel van het DigiD. Daarnaast kent de overheid een opsporingscomponent die ook weer eigen systemen voor het beheren van de identiteiten van (verdachte) burgers kent. De DNA-Databank is hiervan een voorbeeld.

3.2.1 Case: DigiD

DigiD is het door de overheid gebruikte authenticatiesysteem waarmee burgers toegang kunnen krijgen tot veel verschillende diensten bij diverse overheidsinstellingen. Een DigiD-inlogcode bestaat uit een gebruikersnaam en een wachtwoord die de gebruiker allebei zelf samenstelt, om ze makkelijk te kunnen onthouden. DigiD heeft drie verschillende zekerheidsniveaus: Basis, Midden en Hoog. Hoe hoger het zekerheidsniveau van de DigiD, hoe sterker de overheid erop kan vertrouwen dat de persoon achter de gebruikte DigiD ook daadwerkelijk is wie hij zegt te zijn. Het niveau Basis bestaat uit een DigiD-gebruikersnaam met wachtwoord. Daarmee kan een gebruiker bij de meeste overheidsinstellingen terecht. Als bij de DigiD aanvraag ook een mobiel nummer wordt gebruikt met sms-functie, dan is sprake van zekerheidsniveau Midden. De gebruiker kan in die gevallen naast de DigiD-gebruikersnaam en wachtwoord een eenmalige transactiecode intoetsen. Die code ontvangt de gebruiker binnen enkele seconden als sms-bericht op de mobiele telefoon. De code dient als extra controle om de identiteit vast te stellen. In de toekomst zal de elektronische identiteitskaart worden ingevoerd. Met deze elektronische identiteitskaart kan de gebruiker beschikken over zekerheidsniveau Hoog. Voor de meeste elektronische diensten van overheidsinstellingen biedt het basisniveau voldoende zekerheid over de identiteit van de gebruiker. Voor het aanbieden van diensten waar (meer) privacygevoelige informatie wordt uitgewisseld, kan een hoger niveau gewenst zijn. De desbetreffende overheidsinstelling beslist zelf welk zekerheidsniveau gewenst is voor welke diensten die zij aanbiedt.[74]

www.digid.nl

3.2.2 Case: DNA-databank

Sinds in 2005 de Wet DNA-onderzoek bij veroordeelden in het leven werd geroepen, is iedereen verplicht DNA af te staan na een veroordeling voor een misdrijf waarop een straf van minstens vier jaar staat. De gegevens worden twintig jaar bewaard.

Bij een DNA-databank gaat het om een bijzonder soort systeem voor het beheren van identiteiten. Een dergelijke databank bevat namelijk verschillende soorten 'identiteiten'. Identiteiten staat hier met opzet tussen aanhalingstekens. In ons land houdt het

74 Voor een volledig overzicht van aangesloten instellingen zie: < http://www.digid.nl/burger/over-digid/wie-doen-mee/>

Nederlands Forensisch Instituut, het NFI, een DNA-databank bij. Daarin zijn DNA-profielen opgenomen van verdachten en van biologische sporen van onopgeloste zaken. Juist bij deze laatste kun je nog niet spreken van een 'identiteit' omdat er slechts een biologisch spoor beschikbaar is dat (nog) niet gekoppeld is aan een persoon. De profielen van verdachten die worden veroordeeld, worden blijvend in de DNA-databank opgenomen. Het NFI verwijdert de profielen van verdachten die vrijgesproken worden of niet langer verdacht zijn.

De Wet Bescherming Persoonsgegevens is van toepassing op de DNA-databank. Het NFI mag daarom DNA-profielen van mensen die niet verdacht worden, zoals getuigen en nog levende slachtoffers, niet opnemen in de DNA-databank. En volgens de wet moet het NFI, als ze een DNA-profiel verwijdert uit de databank, ook het bij het DNA-profiel behorende celmateriaal vernietigen.

Over de voor- en nadelen van een DNA-databank is nog steeds veel discussie. Voorstanders pleiten ervoor dat de samenleving veiliger zal zijn als ieders DNA in zo'n databank staat. Tegenstanders vrezen voor hun privacy en zijn bang dat rechters DNA als onomstotelijk bewijs gaan beschouwen. Bovendien zijn ze bang dat je al wordt verdacht als je weigert DNA te laten afnemen. Tenslotte zijn er ook praktische problemen. Er is veel meer DNA-analysecapaciteit nodig. Om iedereen in Nederland in beeld te krijgen zou je eigenlijk bij alle bezoekers (zakenlui en toeristen) DNA af moeten nemen.

Nederland heeft in 2005 het verdrag van Prüm ondertekend. De bij het verdrag aangesloten landen hebben het recht om elkaars DNA-databanken te raadplegen. Op 20 februari 2008 is het verdrag voor het gehele Koninkrijk der Nederlanden in werking getreden. Daarmee heeft de Nederlandse DNA-databank officieel een internationale component gekregen.

3.3 De zorg

Juist in de zorg is het van belang om te werken met goede systemen rondom het beheren van identiteiten. Hier gaat het vaak om zogenaamde gevoelige gegevens van patiënten.[75] Deze gegevens zullen een sterkere beveiliging behoeven dan bijvoorbeeld een systeem van een online nieuwswebsite op internet. Dit heeft zijn weerslag op het te gebruiken identiteitsmanagementsysteem.

3.3.1 Case: EPD

De invoering van het landelijk Elektronisch Patiënten Dossier (EPD) moet het mogelijk maken om de medische gegevens van patiënten in een virtueel dossier op te slaan, zodat de medische zorgverleners die toegang hebben tot het systeem allen over dezelfde gegevens beschikken. Het systeem is op het moment van schrijven nog niet operabel. In het regeerakkoord is vastgelegd dat het EPD in 2009 moet worden ingevoerd. De door het kabinet voorgenomen landelijke invoering van het volledige elektronisch patiëntendossier in 2009 is vermoedelijk onhaalbaar. Op onderdelen moet dit echter wel mogelijk zijn, zo blijkt uit antwoorden op Kamervragen van Arda Gerkens van de SP.[76] Momenteel kunnen burgers bezwaar maken tegen opname van hun medische gegevens in het EPD.

De totstandkoming van een EPD is noodzakelijk omdat medische gegevens vaak alleen binnen één ziekenhuis of één huisartsenpraktijk beschikbaar zijn. Met het landelijk EPD worden de gegevens beschikbaar voor alle zorgverleners. De computersystemen van zorgverleners worden daarvoor landelijk gekoppeld. Zo ontstaat het virtuele landelijk EPD.

Het uitwisselen van medicatiegegevens geeft zicht op medicijnen die aan patiënten verstrekt zijn. Specialisten, huisartsen, apothekers en andere zorgverleners kunnen deze informatie opvragen. Zo wordt voorkomen dat een patiënt medicijnen krijgt voorgeschreven die niet samengaan met andere geneesmiddelen die hij of zij ook gebruikt. Met behulp van de huisartswaarneemgegevens kunnen waarnemend huisartsen een samenvatting opvragen van een medische dossier dat afkomstig is van de vaste huisarts. Hierin staat informatie over de belangrijkste gezondheidsproblemen en het medicijngebruik van een patiënt. De vaste huisarts wordt via het landelijk EPD op de hoogte gebracht van de diagnose en verrichtingen van de waarnemer.

75 Het begrip 'gevoelig gegeven' komt uit de Wet bescherming persoonsgegevens (Wbp).
76 Kamervragen II, 15 juni 2007.

De angst bestaat dat elektronische dossiers gemakkelijk te kraken en in te zien zijn door onbevoegden. Om dit te voorkomen worden hoge eisen gesteld aan de beveiliging. Deze eisen zijn landelijk vastgelegd in de eisen voor een goed beheerd zorgsysteem (GBZ). Beveiliging gebeurt op het niveau van de zorgverlener: hij moet zich kunnen identificeren en authenticeren met een UZI-pas[77] (een soort paspoort voor zorgverleners). Maar ook de computers van zorgverleners, de computersystemen van de hele instelling en het landelijk schakelpunt (LSP) dienen aan veiligheidseisen te voldoen. Voldoet een zorgverlener of instelling niet aan de eisen voor een goed beheerd zorgsysteem, dan kan deze niet aansluiten op het LSP. Landelijke elektronische uitwisseling van medische gegevens is dan niet mogelijk. Op deze manier wordt voorkomen dat informatie gemakkelijk te kraken is.

Ook kunnen onbevoegden zo geen toegang tot en inzicht in dossiers krijgen. Bovendien wordt permanent vastgelegd (gelogd) wie de gegevens inziet. Op deze manier is controle achteraf ook mogelijk. De zogenaamde 'zwakke' schakel in de keten is de mens zelf. Journalisten deden zich recentelijk telefonisch voor als medewerkers van een ziekenhuis en wisten daarmee de medische gegevens van enkele patiënten te verkrijgen.[78] Uit recent onderzoek van het College Bescherming Persoonsgegevens en de Inspectie voor de Gezondheidszorg is bovendien gebleken dat medewerkers computers ingelogd aan laten staan als zij van hun werkplek weggeroepen worden.[79]

3.4 Het onderwijs

Binnen het onderwijs wordt in toenemende mate gewerkt aan systemen waarmee studenten en medewerkers door in te loggen met één gebruikersnaam en wachtwoordcombinatie gebruik kunnen maken van meerdere diensten, ook buiten de muren van de eigen hogeschool of universiteit. Daarnaast wordt vaak gebruik gemaakt van digitale leeromgevingen waarbinnen veel verschillende handelingen kunnen plaatsvinden door verschillende mensen. Van deze beide volgt hier een voorbeeld.

3.4.1 Case: Blackboard

Blackboard is een digitale leeromgeving die in Nederland op verschillende universiteiten en hogescholen wordt gebruikt. In principe heeft elke bij de onderwijsinstelling ingeschreven student standaard een account op Blackboard. Inloggen gebeurt dan ook doorgaans met de gebruikersnaam en het wachtwoord dat studenten bij hun inschrijving toegewezen krijgen. Medewerkers die betrokken zijn bij het onderwijs kunnen specifiek toegang krijgen tot de digitale leeromgeving. Het systeem kent verschillende rollen die allemaal verschillende mogelijkheden voor het verrichten van handelingen binnen het systeem kennen. Zo bestaan er de rollen van student, onderwijs-assistenten en docenten.

Studenten die ingelogd zijn op Blackboard kunnen van verschillende opties gebruikmaken. Zo kunnen zij desgewenst extra persoonlijke gegevens invoeren in hun profiel. Zij kunnen bijvoorbeeld hun geslacht aangeven, geboortedatum, onderwijsniveau, website of een persoonlijk telefoonnummer. Daarnaast kunnen zij zich inschrijven bij de digitale variant van de vakken die zij volgen. Eenmaal ingeschreven bij een bepaald vak, is datgene wat mogelijk is afhankelijk van de instellingen die een docent of zijn assistent bij dat vak toestaat. Vaak kan gecommuniceerd worden met de medestudenten en betrokken docenten door het zenden van een bericht. Maar ook biedt Blackboard mogelijkheden om online toetsen af te leggen, werkstukken in te leveren of algemene berichten te plaatsen.

3.4.2 Case: Surfspot

Surfspot is een online aanbieder waar studenten en medewerkers van universiteiten en hogescholen goedkope software kunnen kopen. Een student of medewerker kan daarvoor gebruik maken van de inloggegevens van de universiteit of hogeschool waarbij hij ingeschreven of in dienst is. Door op de site van Surfspot aan te geven bij welke instelling iemand ingeschreven of werkzaam is, wordt een scherm geopend om in te kunnen loggen via het universiteits-, of hogeschoolnetwerk. De inloggegevens van de gebruiker worden door de universiteit of hogeschool zelf geauthenticeerd. Nadat authenticatie heeft plaats-

77 UZI staat voor Unieke Zorgverlener Identificatienummer.
78 Zie hierover: M. Effting, 'Een belletje en alle medische gegevens stonden op de fax', Volkskrant, 13 november 2008.
79 Informatiebeveiliging ziekenhuizen voldoet niet aan de norm, Rapportage van een onderzoek in 2007 door het College bescherming persoonsgegevens en de Inspectie voor de Gezondheidszorg naar de informatiebeveiliging in 20 ziekenhuizen, november 2008.

gevonden kan van de diensten van Surfspot gebruik gemaakt worden. Het aanbod van de producten dat 'in de schappen' ligt is afhankelijk van de (software)licentieregelingen die de hogescholen en universiteiten hebben afgesloten. Surfspot hoeft geen permanente gegevens van gebruikers te beheren, dat gebeurt immers op het niveau van de instelling.

www.surfspot.nl

3.5 Het bedrijfsleven

Het bedrijfsleven als sector als zodanig is uiteraard erg uiteenlopend. Juist vanwege de enorme diversiteit aan mogelijke cases op dit gebied is dit een zeer interessante sector om te bekijken. Omdat er geen ruimte is om allerhande systemen te bekijken, is gekozen voor een relatieve nieuwkomer in het veld die probeert om de hoeveelheid sleutels aan de sleutelbos te verkleinen, een betaalsysteem dat door een groeiend aantal webwinkels wordt ingezet en een systeem waarbinnen gebruik gemaakt wordt van een sterke vorm van authenticatie, namelijk biometrie. Nadrukkelijk moet daarbij gezegd worden dat het niet de bedoeling is om elk systeem in beeld te brengen, maar wel een zo breed mogelijk beeld te schetsen van de situatie in ons land.

3.5.1 Case: OpenID

OpenID is een identiteitsmanagementsysteem dat ontstaan is vanuit de gedachte dat het voor gebruikers lastig is om verschillende aangemaakte identiteiten van verschillende websites te onthouden. Via OpenID kunnen bepaalde van deze deelidentiteiten bij elkaar worden gebracht om via één ingang toegang te verkrijgen tot meerdere websites. OpenID is een wereldwijde toepassing, maar bezit ook een specifieke tak die op de Nederlandse markt gericht is.

OpenID is een protocol dat werkt met een zogenaamde 'single sign on'; één punt waar een gebruiker kan inloggen om toegang te krijgen tot meerdere diensten. Het protocol is decentraal opgezet, wat betekent dat er geen centrale server bestaat waarop alle gegevens van de gebruikers bij elkaar worden opgeslagen. Een gebruiker kan zich inschrijven bij een van de vele aanbieders van OpenID; deze aanbieders moeten voldoen aan een bepaalde set eisen die standaard zijn voor alle aanbieders wereldwijd. In principe kan daardoor iedereen aanbieder worden van OpenID. De gebruiker van OpenID kan zijn identiteit overigens altijd meenemen naar een andere aanbieder van OpenID.

Om gebruik te kunnen maken van OpenID moet een gebruiker eerst een account aanmaken bij een aanbieder die hij vertrouwt. Daar kunnen naam, wachtwoord en eventueel wat extra gevens worden ingevuld. De gebruiker krijgt vervolgens een unieke URL. Deze URL kan gebruikt worden om in te loggen bij diensten die gebruikmaken van OpenID. De dienst/website waarop je wilt inloggen, stuurt de gebruiker door naar zijn eigen OpenID-aanbieder. Nadat de gebruiker daar ingelogd heeft, kan aangegeven worden welke gegevens zichtbaar mogen zijn voor de dienst waarbij ingelogd wordt. Daarnaast kan de gebruiker aangeven of bij deze specifieke dienst/website eenmalig, altijd of niet ingelogd mag worden.

www.mijnopenid.nl
www.openid.net

3.5.2 Case: iDEAL

iDEAL is een betaalmethode op internet waarbij verschillende banken zijn aangesloten. Een online winkel kan voor het afhandelen van betalingen van klanten gebruikmaken van de diensten van iDEAL. Als een klant een product wil afrekenen wordt deze via de website van de verkopende winkel doorverwezen naar iDEAL. In een apart geopende site van iDEAL kan de klant vervolgens via zijn eigen bank een online betaling verrichten. De verkopende online winkel hoeft daarvoor geen betalingsgegevens van haar klanten bij te houden. Dit alles wordt door iDEAL geregeld. Voor het betalen van online aankopen hoeft een klant zich niet apart te registreren omdat gebruikgemaakt wordt van de relatie van de klant en de eigen bank. Nadat de klant een betaling via zijn bank heeft goedgekeurd, worden de naam van de klant en het rekeningnummer aan de webwinkel verstrekt. iDEAL werkt momenteel alleen voor betalingsverkeer tussen Nederlandse banken en webwinkels.

www.ideal.nl

3.5.3 Case: Schiphol Airport: Privium

Het Privium-system op Schiphol maakt gebruik van biometrische kenmerken om mensen te herkennen. Door gebruik te maken van het Privium-systeem kunnen reizigers het 'wachten in de rij' op het vliegveld

overslaan. Privium maakt gebruik van een irisscan, een vorm van biometrische identificatie. Wanneer een persoon deelneemt aan Privium worden opnamen gemaakt van beide ogen. Na de scan worden de irisdetails op de chip van een persoonlijke Privium Card opgeslagen. Bij de grenspassage worden de gegevens van de scan in de chip vergeleken met die van het oog. Daarna worden de gegevens direct uit de apparatuur verwijderd. Voor de automatische grenspassage wordt via een systeemkoppeling dezelfde informatie aan de Koninklijke Marechaussee doorgegeven als de informatie die bij een reguliere paspoortcontrole bij de grens gebruikt wordt. De biometrische informatie is op de chip van de Privium Card opgeslagen en niet in een database. Bovendien zijn bij automatische grenspassage het Schiphol-netwerk en het Koninklijke Marechaussee-netwerk volledig van elkaar gescheiden en wordt geen enkele vorm van informatie door beide systemen met elkaar uitgewisseld. Fraude is nooit geheel uit te sluiten, maar een irisscan is zeer fraudebestendig omdat een iris een uniek biometrisch kenmerk is.

www.schiphol.nl/privium

Biometrie: waarde voor identificatie
Biometrie is niet een tovermiddel waarmee iemands identiteit met zekerheid kan worden vastgesteld. Waar het bij biometrie om gaat is dat door het gebruik ervan op bijvoorbeeld een reisdocument kan worden vastgesteld of iemand de rechtmatige houder is van dat document. Of het reisdocument de werkelijke identiteit van de houder bevat valt daarmee niet te beantwoorden.[80] Daarnaast kan worden getwijfeld aan de effectiviteit van het middel. Uit onderzoek is gebleken dat vrij regelmatig onterechte weigeringen of onterechte herkenningen voorkomen. De Leeuw geeft hiervoor als mogelijke redenen dat nog onbekend is in hoeverre externe factoren van invloed zijn op de prestaties van de biometrische technologie. Daarnaast kunnen fysieke en maatschappelijke omgevingsfactoren een rol spelen.[81]

Biometrische processen kunnen onderhevig zijn aan fraude. De Leeuw geeft hiervan een aantal voorbeelden. In het geval van reisdocumenten kan iemand die een sterke gelijkenis heeft met de officiële houder van het document, proberen dit document te gebruiken. Als daarbij een familierelatie bestaat, dan is de kans groter dat hij of zij door de biometrische controle heenkomt. Sabotage is mogelijk door de eigen biometrische kenmerken of de chip te verminken. Daarom moet bij controle worden teruggevallen op de 'fall back' procedure; handmatige controle. Verschillende vormen van afwijkend gedrag, zoals het produceren van grimassen, kunnen de biometrische controle frustreren. En er kan *spoofing* toegepast worden; een biometrisch kenmerk fingeren door bijvoorbeeld een gelatinevlies te gebruiken dat voorzien is van een vingerafdruk.[82]

3.6 Het sociale leven

Het internet is steeds socialer geworden en online weten veel mensen elkaar inmiddels te vinden. Sociale interactie vindt dan ook veelvuldig plaats. Ook in sociale online werelden is sprake van het beheren van identiteit. In deze werelden liggen echter veelal andere zaken ten grondslag aan het beheer van identiteit dan in de meer 'serieuze' sectoren. Zo is het feitelijk niet altijd belangrijk dat identiteit consistent is, kan er veel meer geëxperimenteerd worden en heeft de gebruiker veel meer de eigen hand in het beeld dat hij over zichzelf naar buiten brengt. Meestal kan hij dan ook zelf zijn virtuele identiteiten beheren. Eventuele onmogelijkheden en vraagstukken rondom het beheer van identiteiten in een sociale online wereld komen in hoofdstuk 5 aan de orde, waar de verschillende vraagstukken op het gebied van identiteitsmanagement aan bod komen.

3.6.1 Case: Hyves

Hyves is een sociale netwerksite. Gebruikers van Hyves kunnen via de site hun sociale contacten onderhouden. Om een eigen Hyves account aan te maken, kun je door iemand anders uitgenodigd worden of jezelf via de

80 Zie hierover: De Leeuw 2005, p. 6.
81 De Leeuw 2005, p. 7.
82 De Leeuw 2005, p. 8.

website aanmelden. Na aanmelding kan direct een profiel worden ingevuld en verder aangemaakt. Een profiel kan een enorme hoeveelheid aan persoonlijke informatie bevatten vooral omdat de gebruiker vrij is om allerhande extra informatie toe te voegen via zogenaamde 'blank fields'. Dus, naast een veelheid aan informatie als allerhande persoonlijke gegevens, voorkeuren voor bepaalde merken, hobby's, favoriete boeken/films en een profielfoto, kan de gebruiker ook altijd nog een extra persoonlijke draai aan zijn profiel geven. Als het profiel eenmaal aangemaakt is, kan het uitnodigen van zogenaamde vrienden beginnen. Een lijst met toegevoegde vrienden is te vinden op de profielpagina van de gebruiker.

Op de profielpagina kan de gebruiker foto's plaatsen, filmpjes, gadgets (waaronder filmpjes van YouTube), een blog bijhouden en een zogenaamd 'wie, wat, waar' invullen. De 'wie, wat, waar'-functie geeft een korte omschrijving van datgene waar de persoon zich op dat moment mee bezighoudt en de plaats waar hij dat doet. Eigenlijk is het een soort micro-bloggen wat lijkt op Twitter.[83] Andere gebruikers kunnen krabbels (korte berichtjes) plaatsen op de profielpagina. Daarbij kan niet alleen tekst, maar ook een filmpje of foto geplaatst worden. Gebruikers kunnen ook nog 'getikt' worden door hun vrienden. Een tik is een korte zin waarin een vriend aan een ander bijvoorbeeld zijn genegenheid, afschuw of vriendschap kan uitspreken. De tikken verschijnen ook op de profielpagina.

Hyves biedt de gebruiker verschillende mogelijkheden om bepaalde gegevens af te schermen. Zo kan de gehele profielpagina afgeschermd worden zodat die bijvoorbeeld alleen zichtbaar is voor vrienden. Zichtbaarheid kan op Hyves op verschillende niveaus plaatsvinden: iedereen kan het profiel zien, alleen Hyvers, alleen vrienden van vrienden, alleen vrienden of niemand. Een tamelijk recente uitbreiding van de mogelijkheden tot afscherming van persoonlijke gegevens is het verdelen van de vrienden in bepaalde groepen. Daarmee kan een gebruiker bepalen dat sommige informatie slechts zichtbaar is voor een bepaalde groep van zijn vrienden of wellicht juist niet zichtbaar mag zijn. Vooralsnog is deze optie niet toepasbaar op alle informatie die op een persoonlijke Hyves-pagina te vinden is.

www.hyves.nl

3.6.2 Case: LinkedIn

LinkedIn is ook een zogenaamde sociale netwerksite. Echter, in tegenstelling tot Hyves, is LinkedIn primair gericht op het onderhouden van een zakelijk netwerk. Bij LinkedIn bevat een profiel daarom ook puur professionele informatie. Om gebruik te kunnen maken van LinkedIn moet men eerst een account aanmaken. Daarbij moet informatie gegeven worden zoals naam, e-mailadres, land, postcode, een korte opsomming van de professionele achtergrond en een wachtwoord. Als deze registratie gelukt is, kan het profiel aangemaakt worden. De in het profiel opgenomen informatie kan beperkt worden tot de informatie die al eerder gegeven werd bij het aanmaken van de account. LinkedIn geeft echter wel aan dat jouw professionele identiteit beter naar voren komt naarmate je meer informatie over jezelf verstrekt. Het profiel kan onder meer informatie vermelden over opleidingen, werkervaring en iemands zakelijke specialisatie. Daarnaast kan contactinformatie opgenomen worden en kan aangegeven worden op welke vlakken iemand contacten wil leggen. Zo kan je aangeven dat je geïnteresseerd bent in een nieuwe baan, sprekersmogelijkheden of het 'herontmoeten' van collega's waar je ooit mee hebt gewerkt. Als de gebruiker dit wil, kan ook een foto in het profiel worden opgenomen.

Vervolgens kan de LinkedIn-deelnemer binnen het netwerk zoeken naar bekenden uit het professionele leven. Ook bestaat de mogelijkheid om uitnodigingen te versturen naar mensen die nog geen profiel op LinkedIn hebben. Deze collega's, zakenpartners, mensen uit dezelfde werkkring etc., kunnen uitgenodigd worden als 'connectie'. De uitnodiging moet een referentie bevatten waarin staat waarvan de twee personen elkaar kennen. Na bevestiging door de uitgenodigde is het contact gelegd. Iemand kan een uitnodiging ook afslaan door aan te geven dat hij of zij de persoon die contact zoekt niet kent. In dat geval kan in de toekomst niet weer een uitnodiging naar die persoon uitgaan. De mogelijkheid tot het leggen van contact is daarmee afgesloten. De lijst

83 <http://twitter.com/>.

van iemands contacten is in beginsel zichtbaar voor de mensen die in die lijst zijn opgenomen. De gebruiker kan er echter voor kiezen om zijn contactenlijst af te schermen zodat voor niemand zichtbaar is wie zich in zijn netwerk bevinden. Naast het profiel en een lijst van iemands contacten, kunnen ook recommendations (aanbevelingen) worden opgenomen. Huidige collega's of mensen waarmee in het verleden is samengewerkt kunnen door middel van een korte beschrijving de gebruiker aanbevelen.

www.linkedin.com

3.7 Trends in identiteitsmanagement

In de voorgaande paragrafen zijn veel verschillende soorten identiteitsmanagementsystemen en manieren voor het beheren van identiteiten aan bod gekomen. Het beeld dat daarmee geschetst is, is zeer breed. Het lijkt erop dat er vrij grote verschillen zitten in de manier waarop met identiteiten wordt omgegaan. Ten dele is dit waar. Zoals aangegeven, heeft dit onder meer te maken met het feit dat elke sector zijn eigen behoeften kent en daardoor een eigen manier heeft om identiteiten te beheren. Soms zijn de belangen ook zo op zichzelfstaand dat er vanwege de bijzondere omstandigheden geen andere keuze mogelijk is. Denk daarbij bijvoorbeeld aan de DNA-databank waarin de gegevens van verdachten zijn opgeslagen of het betaalsysteem iDEAL. Afgezien van deze zeer specifieke gevallen zijn er toch bepaalde, meer algemene trends en ontwikkelingen te zien die richting geven aan de ontwikkelingen op het gebied van identiteitsmanagement.

De gebruiker centraal

De gebruiker gaat een steeds centralere plaats innemen. Dit ligt in lijn van de ontwikkelingen op het gebied van web 2.0 en de opkomst van het sociale web. Dat zie je ook terug in de omgang met identiteit en de gedachten daarover. Het user centric identiteitsmanagement vindt steeds meer zijn plaats en wordt ook vaker als uitgangspunt gebruikt bij de ontwikkeling van identiteitsmanagementsystemen.

Meerdere identiteiten in één systeem

Omdat de gebruiker steeds centraler staat, is er ook steeds meer aandacht voor zijn behoeften. Het verkleinen van de wir-war aan verschillende deelidentiteiten en de bijbehorende manieren om toegang tot diensten te verkrijgen staan hoog op de agenda. Naast het hier al aangehaalde OpenID bestaat er bijvoorbeeld momenteel een initiatief om tot een consumentenidentiteit te komen. EazyID wil een landelijk authenticatieplatform oprichten voor de consumentenmarkt. Een consument kan dan door middel van zijn EazyID inloggen bij meerdere aangesloten dienstverleners.[84] Daarmee proberen verschillende spelers op de markt de spreekwoordelijke sleutelbos van gebruikers te verkleinen.

Ook verschillende initiatieven om de sociale deelidentiteiten van gebruikers samen te brengen lopen mee in deze trend. Zo heeft Google het zogenaamde Open Social ontwikkeld, een standaard voor applicatieontwikkeling. Derden kunnen daarmee een bepaalde applicatie ontwikkelen die gebruikt kan worden binnen de online werelden van de aangesloten aanbieders. Zo kan bijvoorbeeld een link worden gelegd tussen de verschillende sociale werelden en de diverse identiteiten die iemand daarbinnen onderhoudt. Onder andere Hyves en LinkedIn zijn al aangesloten gebruikers.[85]

Hergebruik van bestaande systemen

De behoefte om bestaande sleutelbossen te verkleinen betekent niet altijd dat er nieuwe systemen ontwikkeld worden voor het beheer van meerdere identiteiten onder één noemer. Steeds vaker gaan er stemmen op om bestaande middelen in te zetten voor een breder doel. Daardoor worden bijvoorbeeld bestaande authenticatiemiddelen gedeeld of zoekt men naar manieren om deze middelen te delen. Soms hoeft het wiel namelijk niet opnieuw uitgevonden te worden.

84 <https://www.diginotar.nl/Producten/Authenticatie/EazyID/tabid/610/Default.aspx>
85 Voor een volledig overzicht van aangesloten dienstenaanbieders zie: <http://code.google.com/apis/opensocial/partners.html>.

4 Wederzijdse belangen rondom identiteitsmanagement

In dit hoofdstuk wordt nader bekeken welke belangen er nu spelen rondom het managen van identiteiten en de keuzes voor bepaalde systemen. Daarbij wordt eerst specifiek gekeken naar de verschillende belangen van de partijen die betrokken zijn bij identiteitsmanagement. Vaak blijkt echter dat de verschillende belangen heel goed samen kunnen gaan. Op welke vlakken deze verschillende belangen (kunnen) samenkomen leest u in de laatste paragraaf van dit hoofdstuk. De keuze voor een bepaalde aanpak of voor een bepaald systeem is afhankelijk van verschillende belangen. Niet altijd zal aan elk belang een even zwaar gewicht kunnen worden gegeven. Toch bestaan er verschillende mogelijkheden om systemen in te richten die recht doen aan een veelheid van verschillende – en wellicht ook uiteenlopende belangen.[86]

4.1 De belangen van het individu/ de gebruiker

De gebruiker heeft een aantal verschillende belangen die vaak met elkaar te maken hebben en in het verlengde van elkaar gezien kunnen worden. Zo zal gebruiksgemak vaak prevaleren. Daarbij wegen verschillende aspecten mee. Op het moment van schrijven bestaat de situatie dat een gebruiker voor bijna alle diensten waar hij gebruik van (moet) maken een aparte deelidentiteit moet aanmaken. Het aanmaken van die veelheid aan identiteiten gaat voor hem vaak met enig ongemak gepaard.[87] Ten eerste moet de gebruiker telkens opnieuw allerlei (persoonlijke) gegevens invullen. Wie ben ik, waar woon ik, wat is mijn factuuradres, wat is het afleveradres, wat is mijn telefoonnummer, wat is mijn e-mailadres, etc. Daarnaast heeft de gebruiker door die veelheid aan deelidentiteiten ook nog eens te maken met een hele volle 'sleutelbos': voor elke dienst een aparte gebruikersnaam en een apart wachtwoord. En dat moet vervolgens allemaal weer onthouden worden. Zo waren begin 2008 590.000 mensen hun DigiD vergeten. GBO Overheid, die het beheer van DigiD in handen heeft, wijt dit aan het feit dat mensen hun DigiD maar zo weinig hoeven te gebruiken.[88] Ook wordt vaak eenzelfde wachtwoord gekozen (indien er sprake is van een vrije keuze) zodat het allemaal 'wat makkelijker te onthouden' is. Uit recent Amerikaans/Brits onderzoek blijkt dat bijna de helft van de internetgebruikers toegeeft slechts één wachtwoord te gebruiken voor alle diensten waar ze gebruik van maken.[89] Ook Nederlanders blijken voor gemak te kiezen. Uit Europees onderzoek uit 2007 blijkt dat de naam van een huisdier op nummer 1 staat als meest gekozen wachtwoord. Bijna een kwart van de ondervraagden gebruikt altijd hetzelfde wachtwoord en 43 procent van hen geeft aan een eenmaal gekozen wachtwoord nooit meer te wijzigen. Nederlandse internetgebruikers blijken iets beter om te gaan met hun wachtwoorden. Eén op de vijf Nederlandse internetters geeft aan altijd eenzelfde wachtwoord te gebruiken.[90] Zowel het gebruiken van maar één wachtwoord als het nooit wijzigen daarvan kan een gevaar opleveren voor de veiligheid van transacties. Een kwaadwillend persoon hoeft dan namelijk maar één keer een wachtwoord te achterhalen en heeft daarmee toegang tot praktisch alle diensten die de gebruiker afneemt. Daarmee ligt ook het gevaar van identiteitsfraude op de loer.

Gebruiksgemak is niet de enige motivatie voor het verkleinen van die spreekwoordelijke sleutelbos. Als we online communiceren en we doen dit herhaaldelijk met dezelfde virtuele identiteit, dan bouwen we een bepaalde reputatie op. Zo kunt u daarbij denken aan het reputatiesysteem van online verkoopsite eBay. Hoe vaker iemand zaken doet, hoe meer reputatie iemand opbouwt doordat hij (positieve of negatieve) feedback krijgt van de mensen met wie hij online heeft gehandeld. Stel dat diezelfde persoon online zou willen handelen bij een andere dienst. Dan moet hij daar weer opnieuw een identiteit aanmaken en wederom aan het opbouwen van zijn reputatie werken. Een wens van gebruikers kan daarom zijn om die opgebouwde reputatie mee te kunnen nemen zodat zij niet steeds opnieuw onderaan hoeven te beginnen. Daarnaast kan het voor gebruikers ook van belang zijn om hun repu-

86 Zie hierover ook: Jøsang et al 2007, paragraaf 8.
87 C.Y. Johnson, 'Identity crisis. Can you avoid becoming a piecemeal collection of user names, passwords, and online personas?', *The Boston Globe*, 5 mei 2008.
88 T. Sanders, '590.000 Nederlanders vergeten wachtwoorden DigiD', *Webwereld*, 4 april 2008.
89 P. Van Leemputten, 'Surfers gebruiken vaak maar één wachtwoord. Slechts 7 procent neemt extra maatregelen', *ZDNET*, 18 april 2008.
90 A. Van Elburg, 'Naam huisdier meest gebruikte wachtwoord', *Webwereld*, 17 oktober 2007.

tatie niet alleen in de gaten te houden, maar ook te wijzigen als er iets niet klopt of als een zoektocht door middel van Google of wieowie.nl vervelende resultaten oplevert. Online reputatie blijkt steeds belangrijker te worden, althans steeds meer mensen worden zich bewust van de gevolgen van negatieve reputatie.[91]

Toch zal die gebruiker niet altijd willen dat hij nog maar één of slechts enkele virtuele identiteiten heeft. Net zoals iemand in de offline wereld bepaalde kringen waarin hij verkeert van elkaar gescheiden wil houden, zal dat ook een behoefte in de online wereld zijn. Op dit moment is het scheiden van verschillende kringen van iemands identiteit en de daaraan hangende groepen van personen vaak lastig te realiseren. De online wereld bestaat bij de gratie van linkbaarheid. Het koppelen van verschillende deelidentiteiten is daardoor vaak vrij gemakkelijk. In het navolgende hoofdstuk wordt dieper ingegaan op deze problematiek. Voor dit moment volstaat de constatering van dit punt.

4.2 De belangen van het bedrijfsleven

Ook voor het bedrijfsleven bestaan verschillende – met elkaar verbonden – belangen rondom identiteitsmanagement. Ten eerste levert het hebben van een goed werkend identiteitsmanagementsysteem voor het bedrijf gebruiksgemak op. Het gemak bestaat bijvoorbeeld uit het goed op orde hebben van de klantgegevens en de geschiedenis van een klant omtrent zijn gebruik van een dienst. Daardoor kan gemakkelijker 'zaken gedaan' worden. Als de klantgegevens up-to-date worden gehouden kan dit in combinatie met het dienstenafnemingsverleden waardevolle informatie voor het bedrijf opleveren. Ook kan dit leiden tot betere klantenbinding. Klanten kunnen immers op maat bediend worden (gepersonaliseerde dienstverlening). Bovendien hoeven zij niet meermaals gegevens in te voeren, wat weer leidt tot grotere klanttevredenheid.

Klantvertrouwen is een hiermee verwant onderdeel. Wil er sprake kunnen zijn van een succesvolle dienstverlening, dan zal een klant er ook vertrouwen in moeten hebben dat een onderneming zijn zaakjes op orde heeft. Uit onderzoek in 2007 is gebleken dat Nederlanders het vertrouwen dat zij hebben in ondernemingen koppelen aan veiligheid van de systemen van die ondernemingen. 67% van de Nederlanders geeft aan dat onbetrouwbare ICT (en daardoor mogelijk niet veilige systemen) een negatieve invloed heeft op het vertrouwen. Ruim de helft van de Nederlanders geeft daarom aan dat een veilige en betrouwbare omgeving als belangrijk tot zeer belangrijk wordt ervaren met betrekking tot het versterken van het vertrouwen.[92] Ook privacy wordt door een meerderheid van de Nederlandse ondervraagden als een belangrijk aspect genoemd. 56% zegt dat het beschermen van privacy een factor is die het vertrouwen versterkt.[93] Openheid van zaken, transparantie van beleid en duidelijke profilering door middel van het benadrukken van een privacybeleid kunnen daarmee van groot belang zijn voor een aanbieder.

4.3 De belangen van de overheid

Bij de totstandkoming van een elektronische overheid, hoort ook een gedigitaliseerd systeem voor het beheren van de identiteiten van haar burgers. Achterliggende gedachte daarbij is het vereenvoudigen van de dienstverlening door onder meer de mogelijkheid te bieden 'any time, anywhere' gebruik te kunnen maken van overheidsdiensten.[94] De DigiD geeft hieraan invulling door burgers via één identiteit toegang te verschaffen tot verschillende diensten. Denk daarbij ook aan het opsporingsbelang van de overheid. Een voorbeeld daarvan werd gegeven door de case over de DNA-databank van verdachten.

Betere toegankelijkheid en vergemakkelijking van processen kan ook gevonden worden in de wens om niet alleen naar burgers toe voor meer eenheid te zorgen, maar ook voor bedrijven. Daartoe worden dan ook verschillende initiatieven genomen. Het project van ECP-EPN *E-Herkenning voor bedrijven* is daarvan een goed voorbeeld. Het project voorziet in een stelsel voor elektronische herkenningsmiddelen. Met dit stelsel kunnen

91 Zo worden er bijvoorbeeld tips gegeven om ervoor te zorgen dat je reputatie geen schade aangedaan wordt. Zie hierover: Auteur onbekend, '10 tips voor een betere online reputatie', NRC Handelsblad, 13 september 2007.
92 Dit blijkt uit onderzoek dat in opdracht van Unisys werd uitgevoerd in Belgie, Frankrijk, Duitsland, Italie, Nederland, Spanje en Zweden. Voor het onderzoek zie de website van Unisys: <http://www.unisys.nl>.
93 Dit blijkt uit onderzoek dat in opdracht van Unisys werd uitgevoerd in Belgie, Frankrijk, Duitsland, Italie, Nederland, Spanje en Zweden. Voor het onderzoek zie de website van Unisys: <http://www.unisys.nl>.
94 <http://www.e-overheid.nl/>.

bestaande oplossingen voor elektronische herkenning breder ingezet worden. De meeste onderdelen op het gebied van authenticatiemiddelen zijn vaak al aanwezig en kunnen verder worden ontwikkeld.

4.4 Een brug slaan: gedeelde belangen

De verschillende belangen die hier genoemd werden, bestaan niet los van elkaar, maar kunnen elkaar wederzijds beïnvloeden en elkaar behulpzaam zijn. Het is dus van belang oog te hebben voor elkaars belangen en hoe deze met elkaar verenigbaar (kunnen) zijn. Belangen moeten daarbij ook tegen elkaar afgewogen kunnen worden; in het ene geval zal dit belang prevaleren boven het andere. Het gewicht dat aan een belang toegekend wordt, zal daarmee bepalend zijn voor beslissingen over welk identiteitsmanagementsysteem de voorkeur heeft.

Bij de verschillende besproken actoren binnen het beheer van identiteiten zien we een aantal gedeelde waarden. Gemak staat voor zowel aanbieders als gebruikers hoog in het vaandel. Daarbij hoort uiteraard ook de reductie van de hoeveelheid sleutels aan de sleutelbos. Niet alleen gebruikers hebben daar belang bij, ook aanbieders kunnen profiteren van een kleinere sleutelbos doordat zij bijvoorbeeld delen in het gebruik van bepaalde toepassingen. Dit kan weer een administratieve (en dus ook financiële) reductie betekenen. Ook een thema als veiligheid kent een gedeeld belang. Gebruikers willen erop kunnen vertrouwen dat correct met hun gegevens en identiteit wordt omgegaan en aanbieders hebben er belang bij dat hun reputatie op het gebied van veiligheid en beveiliging niet aangetast wordt.

Op het moment van schrijven is de kennis over de stand van zaken van identiteitsmanagement in Nederland binnen de verschillende sectoren nog vrij gefragmenteerd. Kennis over wederzijdse belangen en verwachtingen is daarmee soms ook nog verspreid. Voor een goede werking en totaaloverzicht van de mogelijkheden en onmogelijkheden rond identiteitsmanagement is het daarom belangrijk dat deze informatie bij elkaar komt. Dit is een van de redenen die ECP-EPN stimuleert tot het ontwikkelen van een neutrale plaats waar de verschillende belanghebbenden bij elkaar kunnen komen. ECP-EPN noemt dit een ‘Gezaghebbende Alliantie’. Dit rapport sluit af met een bijlage waarin dit nader onder de aandacht wordt gebracht.

5 Vraagstukken op het gebied van identiteitsmanagement

In de voorgaande hoofdstukken hebben we gezien wat identiteit is en welke verschillende benaderingen er zijn voor een identiteitsmanagementsysteem. Daarnaast werden enkele voorbeelden beschreven van systemen die op dit moment in gebruik zijn in verschillende sectoren in Nederland. Ook kwamen de achterliggende belangen die spelen rondom het managen van identiteiten aan de orde. Daarmee is de basis gelegd voor het nu volgende hoofdstuk. Dit hoofdstuk gaat nader in op de verschillende vraagstukken die leven rondom het managen van identiteit. Zo komen onder meer privacy, veiligheid, standaardisering, identiteitsdiefstal en vertrouwen en reputatie aan de orde.

5.1 Privacy

Het zelf online zetten of verstrekken van allerlei persoonlijke informatie is de afgelopen jaren steeds meer toegenomen. Mensen dragen actief bij aan het ontstaan van zogenaamde digitale voetstappen (sporen) in de online wereld. De informatie die mensen verstrekken is echter wel vaak bedoeld om alleen in een bepaalde context bekend te zijn. Het probleem is dat deze digitale informatie makkelijk uit die specifieke context vandaan gehaald wordt. Daarom is het vaak niet duidelijk wanneer deze informatie geplaatst werd, wat de bedoeling was en voor welk publiek het oorspronkelijk bedoeld is.[95]

Uit Nederlands onderzoek van Ilse Media (2007) blijkt dat de helft van de ondervraagde Nederlanders zich niet zo heel erg druk maakt over wat anderen over hem schrijven. Toch geeft een even grote hoeveelheid van hen aan dat ze wel regelmatig via bijvoorbeeld Google controleren welke informatie er over hen op het web te vinden is. Informatie die mensen over zichzelf plaatsen, blijkt vaak meer aandacht te krijgen. Twee derde van de ondervraagden geeft aan bewust om te gaan met datgene wat ze over zichzelf prijsgeven.[96]

Uit recent Amerikaans onderzoek is gebleken dat mensen wel steeds bewuster zijn van het feit dat in de online wereld veel persoonlijke informatie te vinden is. Van de volwassen internetgebruikers bekijkt in 2007 47% via zoekmachine Google welke informatie er over hen te vinden is. In 2002 was dit nog slechts 22%.[97] Van diegenen die zelf persoonlijke informatie zoeken, geeft 62% aan dat ze niet verrast zijn over datgene wat ze gevonden hebben; 22% van hen had niet verwacht dat er zoveel persoonlijke informatie te vinden was en; 13% was juist verbaasd over het feit dat ze zo weinig informatie over zichzelf op het internet tegenkwamen.[98] Op de vraag of de informatie die ze aantroffen ook correct is, antwoordt 87% dat de meeste informatie klopt (in 2002 was dit 74%). Elf procent van de ondervraagden geeft aan dat het merendeel van de gevonden informatie niet klopt.[99] Ook wordt door één op de vijf ondervraagden gezocht naar werkgerelateerde persoonlijke informatie. 19% geeft aan dat ze hebben gezocht naar informatie over collega's, zakenrelaties of zakelijke concurrenten.[100] Overigens wordt het meest gezocht naar contactinformatie. Bijna driekwart van de ondervraagden geeft aan dat zij daar primair naar zoeken.[101]

Het Amerikaanse onderzoek toont ook aan dat 60% van de ondervraagden zich geen zorgen maakt over de informatie die over hen te vinden is. Zij ondernemen dan ook geen stappen om de hoeveelheid persoonlijke informatie te reduceren. Bijna 38% daarentegen zegt juist wel ingegrepen te hebben om persoonlijke informatie te verminderen.[102] Van degenen die zeggen dat ze zich zorgen maken over de persoonlijke informatie, blijkt dat meer dan de helft van hen geen actie onderneemt en de gewraakte informatie dus gewoon laat staan.[103]

Camenisch et al wijzen erop dat vaak ten

95 Zie hierover: PEW Report *Digital Footprints* 2007, p. 4.
96 Onderzoek 'Digitale Huishoudens', Ilse Media, 2007. Voor het persbericht zie: 'Internetters bewust bezig met hun digitale identiteit', 28 december 2007, <http://www.ilsemedia.nl/en-web-nieuws-persberichten-28122007.php>.
97 PEW Report *Digital Footprints* 2007, p. 7.
98 PEW Report *Digital Footprints* 2007, p. 11.
99 PEW Report *Digital Footprints* 2007, p. 13.
100 PEW Report *Digital Footprints* 2007, p. 26.
101 PEW Report *Digital Footprints* 2007, p. 27. Op pagina 28 van het rapport staat een volledig overzicht van het soort persoonlijke informatie waarnaar gezocht wordt.
102 PEW Report *Digital Footprints* 2007, p. 30.
103 PEW Report *Digital Footprints* 2007, p. 30.

onrechte gedacht wordt dat gebruikers vrijwillig veel informatie verschaffen aan dienstverleners. Hoewel in bepaalde gevallen er wel degelijk sprake is van vrijwillige informatieverschaffing – zoals bijvoorbeeld het geval is in openbaar toegankelijke profielen – hebben zij wel een punt. Zij wijzen namelijk vooral op de hoeveelheid informatie die gebruikers moeten verschaffen op online formulieren. Volgens hen gaat het in die gevallen niet om een vrijwillige en afgewogen keuze van de gebruikers, maar eerder een gedwongen situatie vanwege het gebrek aan alternatieven. Om toegang tot de dienst te krijgen, moeten bijvoorbeeld de verplichte velden op een dergelijk formulier ingevuld worden. Daarnaast wijzen zij op het bestaan van ongelijke machtsverhoudingen. Transactiekosten en onzekerheid over mogelijk misbruik van hun persoonlijke gegevens verhindert gebruikers ervan om hun dienst elders te gaan halen, menen zij.[104]

Privacy is een heet hangijzer voor alle betrokken partijen bij het beheer van identiteit. Gebruikers vertrouwen erop dat zowel de overheid als het bedrijfsleven op een juiste manier met hun identiteit en persoonlijke gegevens omspringt. Privacy en het beschermen van persoonlijke gegevens staan dan ook in nauw verband met veiligheid en beveiliging. Op beveiligingsvraagstukken wordt nader ingegaan in paragraaf 5.4. In het verlengde van privacy en veiligheid van gegevens ligt het vraagstuk van identiteitsdiefstal en identiteitsfraude. Paragraaf 5.3 gaat daar nader op in. Daarnaast ziet privacy ook op het van elkaar gescheiden houden van de verschillende deelidentiteiten van een persoon. Het samenvallen van identiteiten kan problemen opleveren op het gebied van privacy. Het scheiden van de verschillende publieken die bij de verschillende identiteiten horen is dan ook van groot belang. Paragraaf 5.6 besteedt aandacht aan dit scheiden van publieken.

5.2 Mede-gebruik en standaardisering

In de online en gedigitaliseerde wereld bestaan legio mogelijkheden om identiteiten te beheren. Iedere dienst, elke website en elke aanbieder of instelling beschikt over zijn eigen identiteitsmanagementsysteem. In bepaalde gevallen is dit noodzakelijk vanuit veiligheidsoogpunt of vanwege pragmatische redenen. Toch zijn er verschillende gevallen denkbaar waarbij het niet alleen handig, maar juist ook praktisch is om identiteiten en authenticatiemiddelen rondom die identiteiten te delen. Zoals we in het voorgaande al hebben gezien, wordt in de praktijk al op verschillende manieren gebruikgemaakt van de mogelijkheid om te delen. Federatieve systemen zijn daar een duidelijk voorbeeld van. Steeds vaker wordt gewerkt aan het samenvoegen van systemen en hergebruik van bestaande middelen. Verschillende systemen zoals Google's Open Social, maar ook het OpenID-initiatief streven ernaar om meerdere deelidentiteiten te beheren via één beheerssysteem. Ook zoekt men steeds vaker naar wegen om bestaande middelen te gebruiken in een bredere context. Zo streeft het ministerie van Economische Zaken ernaar om in 2009 te komen tot een gezamenlijk gebruik van middelen rondom *E-Herkenning voor bedrijven*.

Wat betreft systemen die privacy-verhogend werken, bestaat helaas nog niet veel standaardisatie en interoperabiliteit.[105] Juist op het gebied van privacy ziet men dat daar ad hoc – dat wil zeggen door de verantwoordelijke voor een systeem – gewerkt wordt aan interne oplossingen om aan de wensen van de gebruiker rond de bescherming van zijn gegevens en identiteit tegemoet te komen.

5.3 Identiteitsdiefstal en identiteitsfraude

In 2006 concluderen Koops en Leenes dat er veel verschillende termen en definities worden gebruikt door even zovele auteurs om aan te geven wat identiteitsdiefstal of identiteitsfraude is.[106] Zij pleitten er daarom voor om te komen tot een eenduidige definitie van deze begrippen. Volgens de auteurs kan identiteitsfraude als volgt omschreven worden: "Identity fraud is fraud committed with identity as a target or principal tool".[107] Identiteitsdiefstal omschrijven zij als: "Identity 'theft' is fraud or another unlawful activity where the identity of an existing person is used as a target or principal tool

104 Camenisch et al 2005, paragraaf 1.1.
105 Camenisch et al 2005, paragraaf 1.1.
106 Koops en Leenes 2006.
107 Koops en Leenes 2006, paragraaf 3.3.

without that person's consent".[108] Zij brengen dit onderscheid aan omdat het in principe niet mogelijk is om iemands identiteit te stelen vanwege het feit dat de identiteit niet verdwenen is uit de beschikkingsmacht van degene om wiens identiteit het gaat. De term *identiteitsdiefstal* zou daarom misleidend kunnen zijn. Waar het er praktisch gezien op neerkomt is dat iemands persoonlijke gegevens of diens identiteit gebruikt worden om ofwel fraude of andere strafbare feiten mee te plegen. In het geval van fraude valt te denken aan het gebruiken van iemands persoonlijke gegevens om bijvoorbeeld producten of diensten aan te schaffen.

Recent is het Centraal Meldpunt Identiteitsfraude opengesteld voor Nederlandse meldingen rondom fraude met identiteiten.[109] Het meldpunt is een initiatief van de overheid en moet in het eerste kwartaal van 2009 haar definitieve vorm gaan krijgen. Identiteitsfraude wordt daar begrepen als: "...het opzettelijk en met of zonder toestemming verkrijgen, toe-eigenen, bezitten of creëren van valse identificatiemiddelen en het daarmee begaan van een wederrechtelijke gedraging." Het meldpunt moet een duidelijker beeld geven hoe groot het probleem van het oneigenlijk gebruik van identiteiten in Nederland is. Vooralsnog zijn daar geen concrete cijfers over bekend. Staatssecretaris Bijleveld van Binnenlandse zaken en minister Hirsch Ballin van Justitie willen deze gegevens gebruiken om beleid te formuleren. Naast het melden van fraude, kan het meldpunt ook ingezet worden waar sprake is van fouten met persoonlijke gegevens. Het meldpunt spreekt van fouten met persoonsgegevens "als registraties in systemen van overheidsdiensten of bedrijven niet overeenkomen met de gegevens op uw identificatiemiddel zoals uw paspoort of rijbewijs."

5.4 Veiligheid en beveiliging

Het aspect veiligheid speelt op verschillende lagen binnen het beheren van identiteit en de persoonlijke gegevens die daarmee gemoeid zijn. Daar waar persoonlijke gegevens verwerkt worden, moet sprake zijn van een adequaat niveau van beveiliging van die gegevens om onder meer te voorkomen dat derden toegang tot deze gegevens kunnen krijgen. Het voorzien in een optimale beveiliging van systemen rondom identiteitsmanagement zal daarmee niet een aspect zijn dat voor eens en voor altijd geregeld kan worden. Veiligheid en beveiliging zijn onderwerpen die doorlopend de aandacht verdienen. Overigens moet hierbij opgemerkt worden dat niet voor elk identiteitsmanagementsysteem eenzelfde niveau van veiligheid zal hoeven gelden. Als met meer gevoelige gegevens van personen wordt gewerkt zal de beveiliging een hoger niveau moeten hebben dan in die gevallen waar slechts gebruik wordt gemaakt van een anonieme identiteit waarmee bijvoorbeeld commentaar op nieuwssites geleverd kan worden.

Veiligheid en beveiliging zijn daarnaast aspecten die vaak in de publieke belangstelling staan. Met enige regelmaat verschijnen in het nieuws negatieve berichten over het 'uitlekken' van klantgegevens of gegevens van burgers. Dergelijke berichten kunnen – afgezien van de gevaren rondom identiteitsfraude en diefstal – ook perceptieproblemen opleveren. De reputatie van degene die deze gegevens beheert staat daarbij op het spel. Maar het negatieve effect in perceptie kan ook verder reiken en in zijn algemeenheid leiden tot het ontstaan van een negatief beeld rondom het beveiligen van gegevens. Dat heeft weer zijn weerslag op het vertrouwen van gebruikers in de aanbieders van diensten. Openheid van zaken zou kunnen zorgen voor een beter begrip bij gebruikers. Dit is één van de redenen waarom op Europees niveau gewerkt wordt aan het realiseren van een meldingsplicht van datalekken via Privacyrichtlijnen. Bedrijven moeten publiekelijk bekend maken als op grote schaal persoonsgegevens in handen van derden zijn gekomen. De Raad van Ministers van de Europese Unie wil de meldingsplicht alleen laten gelden voor telecom- en internetaanbieders. Of een dergelijke meldingsplicht ver genoeg reikt, wordt door sommigen betwijfeld. Zo pleit EU-privacy toezichthouder Hustinx ervoor om deze plicht bijvoorbeeld ook te laten gelden voor online banken en apotheken. Binnen de huidige EU-richtlijn zouden deze buiten de verplichting vallen.[110]

108 Koops en Leenes 2006, paragraaf 4.
109 <http://www.bprbzk.nl/idfraude>.
110 Zie hierover: T. Van Ringelestijn, 'Roep om meldplicht datalekken zwelt aan', Webwereld, 10 november 2008. En ook: T. Sanders, 'EU pleit voor verscherping meldplicht informatielekken', *Webwereld*, 7 juli 2008.

5.5. Vertrouwen en reputatie

Om communicatie tussen partijen goed te laten verlopen is een bepaalde mate van vertrouwen vereist. Zo hebben we bijvoorbeeld gezien in de besproken zienswijze bij identeitsmanagement, dat uitgaat van privacy verhoging, dat zowel de aanbieder als de gebruiker van een dienst er wederzijds vertrouwen in moet hebben dat de aanbieder van de credentials ter zake kundig is. Een dienstenaanbieder zal erop moeten vertrouwen dat een afgegeven credential goed is (niet verlopen of onjuiste informatie bevat). Een gebruiker zal erop moeten vertrouwen dat de derde partij die credentials verstrekt, netjes met zijn gegevens omgaat. In de offline wereld is het makkelijker iemand te vertrouwen tijdens communicatie. Zo kan men bijvoorbeeld letterlijk zien of iemand een betrouwbare verkoper is doordat hij of zij bijvoorbeeld gevestigd is in een winkelpand, bepaalde kleding draagt en ook of andere klanten goed geholpen worden. In de online wereld is het een stuk lastiger om zekerheid te hebben over deze zaken.[111] Nissenbaum stelt dat er verschillende factoren zijn in online omgevingen die vertrouwen in de weg kunnen staan. Ten eerste hoeven mensen in online omgevingen niet hun offline identiteit prijs te geven. Vaak gebeurt communicatie op grond van anonieme of pseudonieme identiteiten. Daardoor nemen de factoren waarop wij ons vertrouwen in anderen baseren, af. In bepaalde gevallen is er ook geen sprake van een zogenaamde 'sustained identity', een identiteit die langere tijd in gebruik is waardoor een bepaalde reputatie met deze identiteit verweven is. Er bestaat in die gevallen geen informatie over ervaringen in het verleden die zouden kunnen aangeven of een bepaalde persoon te vertrouwen is.[112] Vertrouwelijke communicatie is bovendien moeilijker omdat er in de online wereld geen zicht is op iemands uiterlijk, lichaamstaal en gebaren.[113]

Vertrouwen hangt nauw samen met reputatie. Een reputatie is iets dat opgebouwd moet worden. Daarvoor moet een bepaalde identiteit voor een langere periode gebruikt worden (de eerder genoemde sustained identity). In online omgevingen bestaan systemen die reputatie weergeven. Het meest bekende voorbeeld daarvan is het reputatiesysteem van veilingsite Ebay.[114] Iedereen die koopt of verkoopt bij Ebay heeft een feedbackprofiel. Via dit profiel kunnen kopers en verkopers elkaar wederzijds beoordelen. Aan de hand van de commentaren op een bepaalde koper/verkoper worden punten toegekend.

Reputatie kan ook tegen iemand werken. Jeugdige onbezonnenheid op het internet kan in de toekomst wel eens voor problemen gaan zorgen bij sollicitaties. De Britse privacywaakhond, The Information Commissioners Office, heeft zelfs een waarschuwing uit doen gaan over de mogelijk ongewenste effecten van sociale netwerk sites zoals Facebook, Myspace en bijvoorbeeld ook het in Nederland erg populaire Hyves. Uit een enquête van de ICO bleek dat meer dan de helft van de ondervraagde jongeren gemakkelijk persoonlijke informatie via internet prijsgeeft.[115] De angst voor ongewenste zoekresultaten zit er inmiddels aardig in. De Amerikaanse markt speelt hier graag op in door het mogelijk te maken je online reputatie in de gaten te houden en waar mogelijk te herstellen. Een slecht Googleresultaat moet daarmee tot het verleden gaan behoren.[116] Ook de Nederlandse politiek lijkt zich zorgen te maken over de mogelijke gevolgen van de Googledrift van werkgevers. In oktober 2006 pleitten kamerleden Gerkens (SP) en Van Dam (PvdA) er al voor dat de overheid meer moet doen aan voorlichting over deze gevaren. Volgens hen beseffen jongeren niet dat alles wat zij op internet doen, gevolgen kan hebben in hun latere leven.[117]

5.6 Het scheiden van de publieken

In het dagelijks leven 'spelen' wij verschillende rollen. We zijn ouder, klant, patiënt, burger, vriend en nog vele dingen meer. Al deze verschillende deelidentiteiten willen en kunnen we in de offline wereld relatief makkelijk van elkaar scheiden. Op het werk doen we

111 Nissenbaum 2001, p. 114.
112 Nissenbaum 2001, p. 113.
113 Nissenbaum 2001, p. 113.
114 <http://pages.ebay.nl/securitycenter/feedback.html>.
115 M. Gijzemijter, 'Jeugd gewaarschuwd voor sociale netwerken', *Webwereld*, 23 november 2007.
116 Auteur onbekend, 'Websites verwijderen ongepaste zoekresultaten', Webwereld, 7 augustus 2007.
117 M. Reijnders, 'Voorlichting overheid anoniem internetten schiet tekort', Webwereld, 6 oktober 2006. De kamerleden deden hun uitspraken tijdens een deelnemersbijeenkomst van ECP.NL: <http://www.ecp.nl/agenda/id=212/Deelnemersbijeenkomst_ECPNL.html> Voorlichting aan jongeren, maar ook volwassenen en het MKB, over de gevaren van internet vindt inmiddels plaats via het programma Digivaardig & Digibewust.

geen dingen die we in ons privé leven doen en in principe komen de mensen uit ons privé leven ook niet in contact met de mensen die wij op of via ons werk ontmoeten. We scheiden onze verschillende deelidentiteiten. Dit gaat op een vrij natuurlijke wijze. In de online wereld is het vaak lastiger om deze zogenaamde 'audience segregation' (het scheiden van de publieken) te realiseren. De gewenste scheiding speelt op twee verschillende niveaus. Ten eerste bestaat daar de scheiding tussen personen die we zouden willen aanbrengen binnen een bepaalde online sfeer/wereld. Denk daarbij bijvoorbeeld aan de besproken case van Hyves. Hyves kent maar één definitie wat betreft personen die aan de lijst van vrienden worden toegevoegd. Iedereen is 'vriend' en krijgt daarmee meteen toegang tot en inzicht in alle informatie die via het profiel openbaar gemaakt wordt. Het probleem waar mensen tegenaan kunnen lopen is dat zowel je collega's, familie, vage kennissen, mensen uit het professionele netwerk en vrienden zich aan kunnen melden met het verzoek 'vriend' te worden. Vooralsnog bestaat er geen mogelijkheid om deze verschillende mensen uit verschillende kringen van het leven aparte labels te geven. Daarnaast bestaat behoefte aan het scheiden van de verschillende identiteiten van personen op een hoger niveau. Daarbij gaat het om het scheiden van de verschillende rollen van mensen in de online wereld. Ook dit blijkt lastig te realiseren. In de online wereld kunnen makkelijker (letterlijk) links gelegd worden tussen de verschillende rollen van mensen. Zoekmachines als wieowie.nl maken dit vrij eenvoudig.[118] Wieowie.nl doorzoekt verschillende online werelden op informatie over de persoon wiens naam in het systeem ingegeven wordt. Als iemand een niet al te vaak voorkomende naam heeft, kan daarmee al snel een vrij omvattend beeld over die persoon verkregen worden. Zo worden onder meer de gegevens gecombineerd van verschillende sociale netwerk sites zoals Hyves en Facebook, de professionele netwerksite LinkedIn, blogs, zoekresultaten uit Google, en nog veel meer.

118 <http://www.wieowie.nl>.

6 Sectoroverkoepelende visie: conclusies en aanbevelingen

In het voorgaande is uitgebreid aandacht geweest voor de verschillende soorten identiteitsmanagementsystemen die in werking zijn, de vraagstukken die leven op het gebied van het beheer van identiteiten en de belangen die spelen bij de betrokken partijen. Om duidelijk te maken wat nu de stand van zaken is in Nederland werd daarvoor een onderscheid gemaakt in sectoren. In dit hoofdstuk wordt juist de nadruk gelegd op het geheel en op de zaken die de verschillende sectoren en de verschillende partijen die betrokken zijn bij het beheren van identiteit met elkaar gemeen hebben. Daarmee hopen we te ontstijgen aan discussies die apart van elkaar gevoerd worden maar die wellicht beter en constructiever gevoerd kunnen worden door samen te werken, waarbij oog is voor de gedeelde belangen en oplossingen voor eventueel gerezen vraagstukken.

Identiteit is veranderlijk en dynamisch

Identiteit is geen statisch gegeven. Ten eerste is er sprake van een veelvoud aan deelidentiteiten die alle verbonden zijn aan een persoon. Ten tweede is er sprake van continue verandering. Deelidentiteiten liggen niet vast, een persoon verandert en daarmee zal ook de inhoud en reikwijdte van een deelidentiteit aan verandering onderhevig zijn. Het is daarom ook van belang om rekening te houden met dit veranderlijke karakter van identiteiten. Vooralsnog lijkt daarvoor niet zoveel ruimte te zijn. In een technische visie op identiteit is juist vaak sprake van een vaststaande identiteit. Voor veel identiteitsbeheerssystemen bestaat een identiteit uit een set attributen aan de hand waarvan een individu herkend kan worden. Een identiteitsmanagementsysteem zou meer ruimte moeten bieden aan de veranderlijkheid van identiteit door gebruikers meer opties te bieden in het bijstellen van de eigen identiteit daar waar dat nodig is.

Verschillende soorten identiteiten vereisen verschillende behandeling

In de behandeling van de verschillende cases komt duidelijk naar voren dat er een keur aan verschillende soorten identiteiten gebruikt worden. De ene identiteit is meer sociaal gericht, dan weer is een identiteit meer zakelijk of valt de identiteit samen met burgerschap of is het gericht op de relatie bedrijf-klant. Niet alle identiteiten hebben dus dezelfde kwaliteiten en daarmee lijkt het gegeven dat ook niet alle deelidentiteiten op eenzelfde manier behandeld dienen te worden. Dit besef lijkt enerzijds duidelijk aanwezig, juist omdat er veel verschillende systemen naast elkaar bestaan die elk geënt zijn op een bepaalde identiteit en relatie. Anderzijds zien we een trend tot het samengaan van verschillende systemen en/of authenticatiemiddelen die ervoor zorgen dat meerdere deelidentiteiten van een individu onder één ingang gebruikt kunnen worden. Dit kan ertoe leiden dat de verschillende contexten komen samen te vallen. Het is daarom zaak om deze ontwikkelingen goed in de gaten te houden en daar waar nodig zal aandacht moeten zijn om ongewenste samenval te voorkomen. Echter, daarbij moet niet uit het oog verloren worden dat het terugbrengen van de sleutelbos ook juist verlichting kan brengen voor zowel aanbieders als gebruikers. Telkens zal dus een afweging van belangen moeten plaatsvinden waarin aandacht is voor zowel het gebruiksgemak als voor de eventuele privacyproblemen die daaruit voort kunnen komen.

De gebruiker als centraal punt voor identiteitsbeheer

De groeiende aandacht voor identiteit en het beheer ervan heeft er tevens toe geleid dat er steeds meer oog is voor de gebruiker, zijn wensen en zijn behoeften. Dit is ook te zien in de toename van systemen waarin de gebruiker centraal staat. Toch is het niet altijd even gemakkelijk voor de gebruiker om inzicht te hebben in zijn identiteit en de gegevens waaruit deze is samengesteld. Ook de rechten op correctie, inzage en eventuele wijziging van gegevens blijken niet altijd makkelijk uit te oefenen. Echter, niet duidelijk is of de gebruiker ook altijd wel op de hoogte is van de rechten die hij op grond van de Wbp (Wet bescherming persoonsgegevens) kan uitoefenen. Educatie kan daarmee een belangrijk aspect worden, zeker in de komende jaren.[119]

119 De Consumentenbond benoemde tijdens haar presentatie van de 'Tien geboden voor digitale omgang' een 'recht' op educatie als één van de belangrijke speerpunten voor een beter privacybewustzijn. Voor meer informatie over de geboden zie: <http://www.consumentenbond.nl/actueel/waarstaanwijvoor/privacy>. Februari 2009.

Vraagstukken vragen om aandacht

Veel van de benoemde vraagstukken hebben een raakvlak met privacy. Omdat privacy van nature een diffuus begrip is dat contextafhankelijk haar concrete invulling krijgt, is het belangrijk om de verschillende vraagstukken toch apart te identificeren. Aan verschillende zaken wordt momenteel doorlopend aandacht besteed. Veiligheid en beveiliging zijn daarvan het meest evidente voorbeeld; aanbieders van identiteitsmanagementsystemen integreren deze vraagstukken bijna als vanzelf binnen de bedrijfsvoering. De aankomende plicht tot melding van grote datalekken zal wellicht ook bijdragen aan een verscherpte aandacht voor dit vraagstuk. Op het gebied van bepaalde vraagstukken ontbreekt het echter nog aan de nodige concrete informatie. Zeker daar waar het gaat om identiteitsfraude kan nog een duidelijkheidsslag gemaakt worden. De beschikbare informatie is vooral afkomstig van de Verenigde Staten waar al wel veel onderzoek is gedaan naar de verschillende verschijningsvormen van misdaden met of tegen identiteiten en waar ook concrete cijfers beschikbaar zijn over de omvang van het probleem. Vooralsnog ontbreken deze cijfers voor de Nederlandse situatie. Wellicht dat vanuit het Centraal Meldpunt Identiteitsfraude meer concrete cijfers bekendgemaakt kunnen worden wat betreft het aantal meldingen die zij binnen (gaan) krijgen en de aard van de gevallen die bij hen gemeld worden. Voor zowel dit vraagstuk als de andere benoemde vraagstukken geldt onverkort dat deze alle aandacht behoeven in de nabije toekomst. Hoe deze aandacht concreet ingevuld moet worden, zal vooral afhankelijk zijn van het betreffende vraagstuk. Soms is nader onderzoek vereist en soms is educatie het meer geëigende middel.

Gedeelde belangen, gedeelde zorgen en toch een andere invalshoek

Bij de verschillende actoren in het speelveld kunnen dezelfde belangen geïdentificeerd worden. Noties als veiligheid en privacy spelen door de verschillende sectoren heen en worden ook door gebruikers gedeeld als punten van aandacht. Inbreuken op de beveiliging of zaken die tegen het privacygevoel indruisen, worden door alle partijen erkend als belangrijke punten. Echter, elke actor heeft daarbij zijn eigen achterliggende waarden en normen waardoor de invulling van de concrete belangen en de uitwerking op het beheer van identiteiten net weer anders uit kan pakken. Deze ruimte is van essentieel belang omdat het dwangmatig in een bepaalde oplossingsrichting duwen belemmerend kan werken op innovatie en vrije marktwerking. Dit betekent niet dat men niet van elkaar zou kunnen leren. Een open dialoog kan daarom zeker toegevoegde waarde hebben.

Aanbevelingen

Uit het voorgaande is duidelijk geworden dat een aantal zaken nader aandacht verdient. De conclusies laten zien dat naast de noodzaak van het behouden van eigenheid voor bedrijven, instellingen en overheden waar het hun identiteitsmanagementsystemen betreft, er ook sprake is van gedeelde belangen en gedeelde vraagstukken. Juist deze roepen om samenspraak en overleg. Het op nationaal niveau instellen van een overlegplatform waarin al deze vragen aan bod kunnen komen, kan dan ook bijdragen aan een tegemoetkoming van de gerezen vraagstukken. Een dergelijk overlegplatform zou idealiter dan ook vertegenwoordigers moeten bevatten vanuit alle betrokken partijen. Een korte opzet voor hoe een dergelijk platform ingevuld kan worden, vindt u in bijlage 1.

Wat betreft de verschillende vraagstukken die geïdentificeerd werden, kan vooral winst behaald worden door nader onderzoek te doen naar de Nederlandse situatie. Voor verschillende van de gerezen vraagstukken bestaat al een wetenschappelijk kader waaruit geput kan worden. Toch ontbreekt het aan concrete Nederlandse cijfers, zeker daar waar het gaat over vraagstukken op het gebied van fraude of diefstal. Juist deze zijn noodzakelijk om de situatie correct in te schatten en daarop eventueel handelen in te richten. Voor het identificeren van die vraagstukken waarnaar nader onderzoek moet worden verricht kan een overlegorgaan goed van pas komen. Immers, als alle betrokken partijen bij elkaar komen, kunnen zij snel duidelijkheid hebben waar de behoeftes liggen.

Op het gebied van de gebruiker ligt met name educatie voor de hand als noodzakelijke actie. Vooral op het gebied van privacy en ook de rechten die daaraan voor de gebruiker verbonden zijn kan educatie ten dele uitkomst bieden om ongewenste situaties tegen te gaan. Denk daarbij vooral aan

de huidige jonge generatie en haar andere opvattingen over zaken die publiek of gesloten zijn. Aansluiting bij lopende programma's lijkt daarbij de meest aangewezen weg. Zo is het programma Digivaardig & Digibewust goed ingericht om deze zaken te adresseren.

Bijlage 1:

(Met dank aan Jan Wester voor zijn bijdrage)

Een Gezaghebbende Alliantie: samenkomende belangen

De afgelopen jaren hebben we enkele belangrijke ontwikkelingen gezien op het gebied van de informatiemaatschappij. Verschillende verschuivingen in gebruik, toepassing en ontwikkeling hebben plaatsgevonden die alle zijn weerslag hebben op onze visie op de informatiemaatschappij. Waar in voorgaande jaren vooral de technologische ontwikkeling en het werken met ICT centraal stond, is dat nu steeds meer gaan verschuiven naar daadwerkelijk gebruik en het innoveren met ICT. Vooral de rol van gebruikers is daarbij veranderd en meer centraal komen te staan. Een van die thema's die aan belang hebben gewonnen is het bevorderen van 'vertrouwen' door hobbels weg te nemen op het terrein van *Identity Management, Authenticatie & Privacy*. Deze bijlage geeft inzicht in de vraag wat een Gezaghebbende Alliantie (GA) is, hoe een dergelijke Alliantie zou kunnen werken, en welke stappen er nodig zijn om deze te creëren.

Wat is een Gezaghebbende Alliantie? Doel/werkwijze/producten

De ratio achter de Gezaghebbende Alliantie is het besef dat door de voortschrijdende penetratie van ICT in alle economische en sociale processen, de samenleving zelf fundamenteel aan het veranderen is. Dit betreft niet in de laatste plaats ook de institutionele arrangementen en instellingen zoals we die kennen. Deze zijn in brede zin hun functie en effectiviteit aan het verliezen. Consensusvorming op basis van de klassieke belangen (zuilen, klassen etc.), verliest aan kracht en vormt geen afspiegeling meer van de krachten in de huidige maatschappij. Ook de overheid boet meer en meer aan zeggingskracht in en de verdergaande liberalisering van markten stelt haar voor de uitdagende vraag hoe publieke belangen adequaat geborgd kunnen worden. Ook het bedrijfsleven ziet zich steeds meer geconfronteerd met een gedifferentieerde omgeving en onderhoudt een groeiend aantal hybride relaties met partners (concullega's) en klanten (prosumenten).

Een Gezaghebbende Alliantie is een nieuwe manier om tot consensusvorming te komen die ook daadwerkelijk op bestuurlijk niveau impact kan genereren. Uitgangspunten vormen een aantal nieuwe 'gezond verstand' principes:

- In de toekomst zal de informatiemaatschappij steeds meer gebaseerd zijn op gebruiksgedreven, vraaggestuurde modellen waarbij de gebruiker centraal staat.
- De noodzaak tot permanente, incrementele open innovatie neemt toe om met de toenemende dynamiek om te kunnen gaan.
- Organisaties en personen zullen steeds hybrider met verschillende functies en rollen in netwerken opereren.
- Zakelijke en sociale relaties zullen als gevolg daarvan meer en meer gebaseerd zijn op vertrouwen, richtsnoeren/kaders, consensus vanuit "what's in it for us", met zelfregulering en controle door monitoring.

Functies

Om een Gezaghebbende Alliantie, ook daadwerkelijk gezaghebbend te laten zijn, wordt een aantal functies gecombineerd. Het gaat dan om *agenderen, verbinden, onderbouwen en uitvoeren:*

Verbinden: Binnen de GA wordt op basis van gelijkwaardigheid samengewerkt in de vijfhoek van belanghebbenden (zie figuur 1), en dient op basis van urgent of relevant ervaren thema's een duidelijke verbinding met lopende zaken te worden georganiseerd. De activiteiten kunnen zowel een proces, een product of een programma zijn. Deelnemers zijn alleen diegenen die ook daadwerkelijk bijdragen en zelf 'leiderschap' willen tonen.

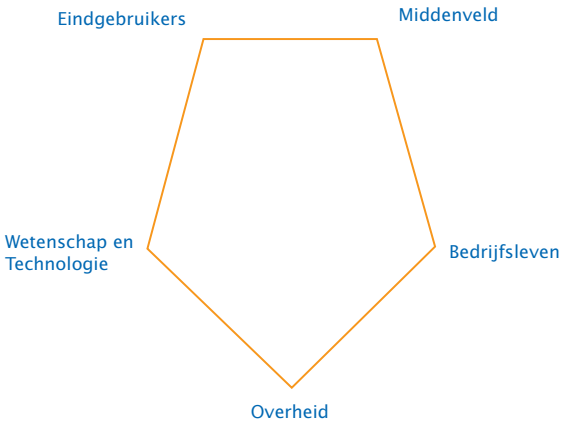
Onderbouwen/uitvoeren: Onder de samenwerking dient een stevig multidisciplinair wetenschappelijk fundament te worden gelegd met neutraal wetenschappelijke instituten als het SCP, TNO, Novay, CBS, etc. Ook moet de mogelijkheid bestaan om de samenwerking in concrete programma's uit te voeren.

Agenderen: Tot slot is het ook zaak met gezag een maatschappelijk agenderende functie in te kunnen vullen. Commitment aan de resultaten op basis van overtuiging is immers bepalend voor het gezag dat daar van uit gaat. Agendering kan plaatsvinden door een ieder waarvan algemeen erkend is dat zij beschikken over natuurlijk gezag en daarbij over het eigen belang heen kunnen kijken.

De verschillende 'bloedgroepen', zoals in onderstaand pentagram weergegeven, die-

nen goed vertegenwoordigd te zijn bij alle drie de functies. Vooral bij de consumenten en het maatschappelijk middenveld, maar ook in het veld van de 'nieuwe media', moet actief worden gewerkt aan tools en middelen om de betrokkenheid van deze groepen te activeren en ECP-EPN als natuurlijke linking point naar de 'oude economie' te positioneren.

Figuur 1. Pentagram van belanghebbenden

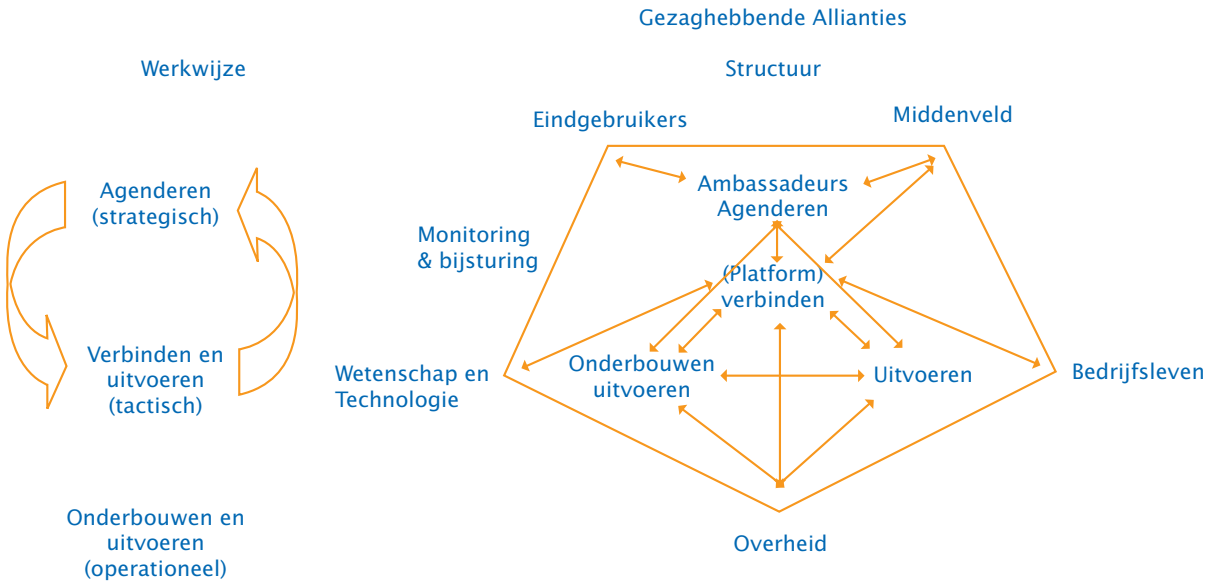


Hoewel een alliantie natuurlijk alleen gezaghebbend is op basis van de resultaten die het bereikt, kan wel een aantal voorwaarden worden geïdentificeerd die de kans op slagen aanzienlijk vergroten. Naast de hierboven genoemde combinatie van functies, is het essentieel om thema's op het juiste niveau te adresseren. Om *agendering, verbinding, onderbouwing* en *uitvoering* te organiseren is het cruciaal dat de thema's herkenbaar zijn en als urgent voor de eigen organisatie worden ervaren. Zo kan onder een abstracte paraplu als **'Vertrouwen'** een verbindend programma **Privacy /ID management en maatschappij** worden ontwikkeld, waaronder vervolgens concrete vraagstukken een uitwerking kunnen krijgen. Bijvoorbeeld op het terrein van **authenticatie** en **publiek-privaat medegebruik**. Hierbij dient steeds te worden bekeken welk type vraagstuk aan de orde is: of het technisch/juridisch, organisatorisch of ethisch van aard is. Vraagstukken worden daarbij primair op basis van inhoud georganiseerd en niet op basis van belangen, waarbij als start steeds de definitie van het "what's in it for us" voorop staat.

Werkwijze

Het volgende organisatiemodel kan dienen om de verschillende functies binnen de Gezaghebbende Allianties te laten functioneren. De basis hiervoor wordt gevormd door onderstaande flowchart.

Figuur 2: Werkwijze



De werkwijze van de Gezaghebbende Alliantie strekt zich uit over de drie niveaus (strategisch, tactisch en operationeel) hetgeen zich vertaalt in de activiteiten *Agenderen, Verbinden, Onderbouwen en Uitvoeren*. Daartoe wordt een *Platform* samengesteld uit representanten vanuit de vijf domeinen. Dit Platform zal een werkwijze kennen van actiegerichte programma's die op zichzelf weer periodiek gemonitord worden teneinde bijsturing mogelijk te maken indien daartoe aanleiding bestaat. Het Platform wordt gevoed en ondersteund door wetenschappelijke instituten die in dit kader samenwerken. Zij toetsen of formuleren vraagstellingen, leggen verbanden en beoordelen uitkomsten (onderbouwing, wetenschappelijke verantwoording, haalbaarheid, schaalbaarheid, uitvoerbaarheid etc.). De ambassadeurs dienen zowel richting Platform als maatschappelijk een agenderende functie te hebben, waarbij het Platform hen van 'body' voorziet. De Platforms worden gefaciliteerd en gehost door ECP-EPN. De rol van ECP-EPN t.a.v. de Gezaghebbende Allianties zal er vooral één zijn van procesfacilitator. ECP-EPN draagt zorg voor een transparant proces rondom de keuze van thema's en geeft vorm aan de verdere operationalisering.

Producten
Een Gezaghebbende Alliantie is in principe zelfsturend. Dat betekent dat ECP-EPN wel een faciliterende rol speelt, maar dat het uiteindelijk de Alliantie zelf is die vaststelt wat er moet gebeuren ten aanzien van de onderwerpen waarvan zij vinden dat die passend zijn binnen de scope van de Alliantie. Concreet komt dit erop neer dat de Alliantie zelf aangeeft welke onderwerpen op de agenda geplaatst dienen te worden en wat daar vervolgens mee gedaan moet worden. Het uiteindelijke product kan daardoor zeer uiteenlopend zijn (een advies, een rapport, een lobby, een samenwerkingsverband, een c*ode of conduct*, etc.).

Meerwaarde voor deelname aan de Alliantie
Waarom is deelname aan de Alliantie van belang en wat is de meerwaarde van een dergelijke alliantie voor de verschillende bloedgroepen?

- De overheid: Een Gezaghebbende Alliantie kan voor de overheid een *bandwagon* vormen waarvan zij kunnen profiteren. De aansprakelijkheid voor bepaalde vraagstukken wordt verzacht.
- Het bedrijfsleven: Als het bedrijfsleven met eigen initiatieven komt, heerst al snel de perceptie dat 'er iets achter zit'. De vooroordelen wat dat betreft kunnen weggenomen worden door deel te nemen aan een Alliantie waarin verschillende partijen plaatshebben.
- De wetenschap: Door deel te nemen aan de Alliantie kunnen zij in hun onderzoek vraaggestuurd gaan werken.
- De gebruikers en het maatschappelijk middenveld: Een Alliantie verzorgt voor deze groepen een duidelijk hoorbare stem.

Literatuurlijst

Anderson 1997
W.T. Anderson, *The Future of the Self*, Penguin Putnam inc: New York 1997

Ardagna et al 2008
C.A. Ardagna, J. Camenisch, R. Leenes, G. Neven, B. Priem, P. Samarati, D. Sommer, M. Verdiccio, 'Exploiting cryptography for privacy-enhance access control. A result of the PRIME project', *PRIME paper*, 2008

Back 1989
K. Back, 'Thriller: The Self in Modern Society', in: J. Shotter and K. Gergen (eds.), *Texts of Identity*, London: SAGE Publications 1989.

Bauman 2004
Z. Bauman, *Identity*, Cambridge: Polity Press 2004

Baumeister 1986
R.F. Baumeister, *Identity. Cultural Change and the struggle for self*, New York: Oxford University Press 1986

Camenisch et al 2005
J. Camenisch, S. Fischer-Hübner, A. Shelat, M. Hansen, J. Tseng, H. Krasemann, D. Sommer, R. Leenes, 'Privacy and identity management for everyone', *DIM'05*, 11 november 2005, Fairfax, Virginia, USA

Clauß & Köhntopp 2001
S. Clauß, M. Köhntopp, 'Identity management and its support of multilateral security', *Computer Networks*, no. 37, 2001, p. 205-219

Cooley 1922
C.H. Cooley, *Human nature and the social order*, Charles Scribner's Sons: New York 1922

Dhamija & Dusseault 2008
R. Dhamija, L. Dusseault, 'The seven flaws of identity management. Usability and security challenges', *IEEE Security & Privacy*, March-April 2008, pp. 24-29

Elliot 2001
A. Elliot, *Concepts of the self*, Polity Press: Cambridge 2001

Frissen & De Mul 2000
V. Frissen, J. de Mul, 'Under construction. Persoonlijke en culturele identiteit in het multimediatijdperk', *Bits of Freedom*, Internet publication, 13 december 2000

Gergen 1991
K.J. Gergen, *The saturated self. Dilemmas of identity in contemporary life*, New York: Basic Books 1991, (the 2000 edition)

Giddens 1991
A. Giddens, *Modernity and self-identity*, Stanford: Stanford University Press 1991

Goffman 1959
E. Goffman, *The presentation of self in everyday life*, 1959 Anchor books

Hansen et al 2004
M. Hansen, P. Berlich, J. Camenisch, S. Clauß, A. Pfitzmann, M. Waidner, 'Privacy-Enhancing Identity Management', *Information Security* Technical Report, vol. 9, no. 1, 2004

Holstein & Gubrium 2000
J.A. Holstein, J. F. Gubrium, *The self we live by. Narrative identity in a postmodern world*, New York: Oxford University Press 2000

James 1890
W. James, *The Principles of Psychology*, chapter 10: 'The Consciousness of Self', 1890, pp. 292-402, available at: <http://psychclassics.yorku.ca/James/Principles/index.htm>

Jøsang et al 2007
A. Jøsang, M. AlZomai, S. Suriadi, 'Usability and privacy in identity management architectures', *AISW 2007*, Ballarat, Australie, 2007

Van Kokswijk 2007
J. van Kokswijk, *Digital Ego. Social and Legal Aspects of Virtual Identity*, Delft: Eburon 2007

Koops & Leenes 2006
B-J. Koops, R.E. Leenes, 'ID theft, ID fraud and/or ID-related crime. Definitions matter'. *Datenschutz und Datensicherheit*, nr. 9, 2006, pp. 553-556

Leary & Price Tagney 2003
M.R. Leary, J. Price Tagney (eds.), *Handbook of Self and Identity*, The Guilford Press: New York 2003

De Leeuw 2005
E. de Leeuw, 'Biometrie in nationaal identiteitsmanagement', *Informatiebeveiliging*, november 2005, pp. 6-10

Mead 1934
G. Mead, *Mind, self and society: from a standpoint of a social behaviorist*, Chicago: University of Chicago Press 1934

Nissenbaum 2001
H. Nissenbaum, 'Securing trust online: wisdom or oxymoron?', *Boston University Law Review*, vol. 81, June 2001, pp. 101-131

Pfitzman & Hansen 2006
A. Pfitzman, M. Hansen, 'Anonimity, Unlinkability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology', version v0.27, 20 February 2006

Prins & Van der Meulen 2006
J.E.J. Prins, N.S. van der Meulen, 'Identiteitsdiefstal: lessen uit het buitenland', *Justitiele Verkenningen*, jrg. 32, nr. 7, 2006

Srivastava et al 2006
Srivastava et al (eds.), *Identity.digital*, ITU Internet report, December 2006

Valkenburg & Jurg 2007
P. Valkenburg, P. Jurg, *Identity Management. Omgaan met elektronische identiteiten*, ICT Bibliotheek 33, Den Haag: 2007

Adres Overgoo 13 Postbus 262 2260 AG Leidschendam **T** +31 (0)70 419 03 09 **F** +31 (0)70 419 06 50
I www.ecp.nl / www.epn.net **Bank** 50 22 75 162 **Stichtingsnummer** 27169301