

ID or not to be?

**Naar een doordacht stelsel voor digitale
identificatie**

© Rathenau Instituut, Den Haag, 2003

Rathenau Instituut
Koninginnegracht 56

Correspondentieadres:
Postbus 85525
2508 CE Den Haag

Telefoon 070 - 342 15 42
Fax 070 - 363 34 88
E-mail info@rathenau.nl
Website www.rathenau.nl

Uitgever: Rathenau Instituut
Eindredactie: Julika Vermolen
Basisvormgeving: Hennie van der Zande, Amsterdam
Opmaak: Henny Scholten, Amsterdam
Grafische productie: Herbschleb & Slebos, Monnickendam
Pre-press en druk: Meboprint, Amsterdam
Bindwerk: Meeuwis, Amsterdam
Vertaling Summary: English Text Company, Den Haag

Dit boek is gedrukt op kringlooppapier

Eerste druk: april 2003

ISBN nummer 90 806772 8 0

Deze publicatie kan als volgt worden aangehaald:
C. Prins en M. de Vries (2003). ID or not to be? Naar een doordacht stelsel voor digitale identificatie. Den Haag: Rathenau Instituut; Werkdocument 91.

Preferred citation:
C. Prins en M. de Vries (2003). ID or not to be? Naar een doordacht stelsel voor digitale identificatie. Den Haag: Rathenau Instituut; Working document 91.

Niets uit deze uitgave mag worden veelevoudigd en/of openbaar gemaakt door middel van druk, fotokopie of op welke wijze dan ook, zonder voorafgaande schriftelijke toestemming van het Rathenau Instituut.

No part of this book may be reproduced in any form, by print, photo-print, microfilm or any other means without prior written permission of the holder of the copyright.

ID or not to be?

Naar een doordacht stelsel voor digitale identificatie

Auteurs:

Prof.mr. Corien Prins is hoogleraar recht en informatisering aan de Universiteit van Tilburg (Centrum voor Recht, Bestuur en Informatisering). In haar onderzoek richt zij zich op de elektronische overheid, e-commerce, privacy en regulering van ICT.

Mr. Marc de Vries BA is toegevoegd senior onderzoeker aan de Universiteit van Tilburg (Centrum voor Recht, Bestuur en Informatisering) en partner bij ZENC BV. Hij schrijft, doceert en adviseert over juridische en beleidsmatige vraagstukken rond e-government en ICT.

Met medewerking van:

Dr. Paul de Hert en Merel Prinsen, beiden ten tijde van dit onderzoek verbonden aan de Universiteit van Tilburg (Centrum voor Recht, Bestuur en Informatisering).

Projectcoördinatie:

Drs. Margot Schoenmacker

Drs. Dirk van Harten

Bestuur Rathenau Instituut

dr. C.J. Kroese (voorzitter)

mw. prof.dr. I. de Beaufort

ir. P.P. 't Hoen

prof.dr. W.K.B. Hofstee

mw. dr.B.E.C. Plesch

mw. mr. J.A. Schaap

prof.ir. E.J Tuininga

prof.dr. W. van Vierssen

dr. D. van Zaane

Voorwoord

Identificatie speelt een belangrijke rol in het dagelijks leven. Regelmatig moeten we aangeven of we de handelingen die we verrichten, ook daadwerkelijk mogen verrichten. Zonder rijbewijs kunnen we geen auto huren; zonder uittreksel uit het bevolkingsregister geen uitkering aanvragen; zonder paspoort niet de grens over, et cetera. Om het identificatieproces zo soepel mogelijk te laten verlopen, zijn meerdere identificatiemiddelen met ondersteunende informatiesystemen in het leven geroepen. Een vrij geoliede machine die tot nu toe nauwelijks problematisch verliep.

Toch vertoont deze machine ook haperingen, onder meer vanwege de toenemende fraudegevoeligheid. Om deze zwakke plekken te bestrijden kan de elektronische snelweg mede een uitweg bieden. De overheid dient hiervoor initiatieven te nemen. Niet alleen om een informatiesamenleving goed op gang te brengen en nieuwe technologieën ten volle te benutten. Het is vooral belangrijk om concrete beleidsambities waar te maken, in het bijzonder ambities die de overheid heeft geformuleerd op het terrein van veiligheid, vreemdelingenbeleid en efficiencyoperaties. Identificatie speelt daarbij een belangrijke rol.

De overheid dient daarom te komen tot een betrouwbaar stelsel van digitale identiteiten en systemen voor identificatie. Het scheppen hiervan raakt onze samenleving in haar fundamenten, waarbij veel belangen spelen die bij de totstandkoming van beleid afgewogen moeten worden. Die overstijging van beleidsterreinen maakt deze materie complex. Bij dit alles hoort uiteraard een scherpe volkstergenwoordiging, die zich realiseert dat een ondoordachte en gefragmenteerde aanpak op termijn nadelige gevolgen zal hebben voor onze samenleving in al haar geledingen.

Deze publicatie beoogt een dergelijke bewustwording te stimuleren en geeft enkele handreikingen aan regering en parlement voor het te creëren beleid. De publicatie schetst een overzicht van relevante beleidsinitiatieven waarin een aantal meta-trends te ontwaren zijn. Vervolgens geeft het een beeld van de keuzes waarvoor we staan en een voorzet voor initiatieven.



Mr. drs. J. Staman
Directeur Rathenau Instituut

Inhoudsopgave

Voorwoord	5
Samenvatting	9
1 Inleiding	13
1.1. Digitale identificatie boeit	13
1.2. Doel van de publicatie	15
1.3. Opzet	15
1.4. Methodiek	15
2 Overzicht van beleidsinitiatieven rond digitale identificatie	17
2.1. Inleiding	17
2.2. Digitale identificatie en vier relevante beleidsthema's voor de toekomst	18
2.2.1. Veiligheid	18
2.2.2. Vreemdelingenbeleid	19
2.2.3. Dienstverlening door de overheid	19
2.2.4. Efficiency van de overheid	20
2.3. De beleidsthema's van de toekomst in relatie tot de initiatieven van nu	20
2.4. Schematisch overzicht van de initiatieven rond digitale identificatie	22
2.5. Analyse van de initiatieven	25
2.5.1. Spraakverwarring	25
2.5.2. Overconcentratie op middelen	25
2.5.3. Smartcards: beperkt succes en niet geïntegreerd	25
2.5.4. Toenemende gebruik van biometrie	26
2.5.5. Gebruik van nummers neemt toe	26
2.5.6. Meerketengebruik van nummers	27
2.5.7. Monopolie van de overheid bij de toekenning van identificatiemiddelen wankelt	27
2.5.8. Naar steeds persoonlijker identificatie	28
2.6. Besluit	29

3	Afwegingen, conclusies en aanbevelingen – een uitruil van belangen	31
	3.1. Inleiding	31
	3.2. Een viertal afwegingen	31
	3.2.1. Infrastructuur: eenheid versus diversiteit	31
	3.2.2. Zwaarte van het middel: absoluut of relatief	32
	3.2.3. Regie: publiek versus privaat	33
	3.2.4. Wens: gemak en resultaat versus vrijheid	34
	3.3. Conclusies en aanbevelingen	35
	3.3.1 De overheid moet volgen	35
	3.3.2 De overheid moet het debat leiden	36
	3.3.3 De overheid moet handelen	38
	3.4. Epiloog	39
	Bijlagen	41
	1. Identiteit, identificatie en middel	41
	2. Overzicht geïnterviewde personen en deelnemers workshop	45
	3. Overzicht beleidsinitiatieven naar initiatiefnemers	47
	Noten	51
	Summary	53
	Literatuur	57
	Internetbronnen	59

Samenvatting

We staan aan de vooravond van enkele beslissingen omtrent de creatie van een stelsel van digitale identificatie. Deze beslissingen zijn dusdanig fundamenteel dat volksvertegenwoordigers de komende jaren veelvuldig te maken zullen krijgen met deze materie. Deze publicatie is bedoeld om het parlement in staat te stellen zich een beter beeld te kunnen vormen van de:

- problematiek rondom digitale identificatie;
- relevante beleidsinitiatieven, hun context en doelstellingen, mede in het licht van huidige politieke ambities;
- keuzes waarvoor we staan en de mogelijke ontwikkelingsrichtingen die zich aftekenen.

Het belang van identificatie

Identificatie is een belangrijk fundament van onze samenleving. Het geeft ons de mogelijkheid een koppeling aan te brengen tussen personen, handelingen en verantwoordelijkheden. De situaties in het dagelijks leven waarin een vorm van identificatie nodig is, zijn talrijk en betreffen contacten met particulieren, bedrijven en de overheid. In veel opzichten vormt identificatie een van de smeermiddelen die maatschappelijk functioneren mogelijk maken. Om het hele proces soepel te laten verlopen, heeft de overheid een identificatiestelsel geschapen. Binnen dit stelsel spelen fysieke identificatiemiddelen (vooral papieren identiteitsdocumenten) nog steeds de boventoon.

Maar de huidige informatiesamenleving vraagt om digitale equivalenten van de fysieke vormen van identificatie. Zonder een goed functionerend stelsel van digitale identificatie zal bijvoorbeeld de criminaliteitsbestrijding ernstig worden bemoeilijkt, zullen ambities op het gebied van een elektronische overheid worden gefrustreerd, zullen bedrijven en burgers vertrouwen missen in *e-commerce* activiteiten en zal uiteindelijk onze concurrentiepositie verslechteren. Het is daarom noodzakelijk na te denken over de vormgeving van een digitaal identificatiestelsel.

Voor de regering vormt digitale identificatie een belangrijk aanknopingspunt om maatregelen te treffen op het gebied van veiligheid, vreemdelingenbeleid, dienstverlening door de overheid en efficiency van de overheid. Digitale identificatie staat dan ook de komende periode prominent op de beleidsagenda. De regering die in 2003 aantreedt zal naar verwachting de ingezette koers voortzetten, hoewel opvalt dat het perspectief zeer eenzijdig is geworden: de huidige

discussie gaat vooral over de rol die identificatie speelt voor het veiligheids- en het vreemdelingenbeleid.

Trends

Uit een overzicht van de belangrijkste Europese en Nederlandse beleidsinitiatieven waar identificatie een rol speelt komt een aantal duidelijke trends, gemeenschappelijkheden en opmerkelijkheden naar voren:

- er heerst een grote spraakverwarring: de terminologie in verschillende beleidsdocumenten is verre van consistent;
- er bestaat een overconcentratie op de middelen: er is nauwelijks aandacht voor de processen rond (management van) identificatie;
- de experimenten met smartcards zijn een beperkt succes en voorlopig nog niet geïntegreerd;
- het gebruik van biometrische kenmerken voor identificatiedoelinden neemt toe;
- ook het gebruik van nummers neemt toe, hoewel daar nog geen eenheid in systeem aan ten grondslag ligt;
- dezelfde nummers worden voor meerdere doeleinden gebruikt (meerketengebruik);
- het monopolie van de overheid bij de toekenning van identificatiemiddelen wankelt;
- de identificatiemiddelen worden steeds meer op de persoon toegesneden, tot nagenoeg een allesomvattend beeld van iemands identiteit.

Wat betekenen deze trends? Welke fundamentele vragen roepen ze op? Waar zal de komende jaren op moeten worden gestuurd? De hier gesignaleerde trends roepen vier fundamentele vragen op, te weten:

1. De infrastructuur: eenheid versus diversiteit

Er is behoefte aan mogelijkheden om de verschillende initiatieven te coördineren en waar mogelijk op elkaar af te stemmen of te integreren. De uiterste variant van integratie is een uniform stelsel voor digitale identificatie. Echter, met elke stap die de overheid in die richting zet, maakt ze de samenleving ook afhankelijker van het adequaat functioneren van dat ene stelsel en wordt de burger kwetsbaarder.

2. De zwaarte van het middel: absoluut of relatief

Een tweede afweging is de vraag hoe sterk het identificatiemiddel moet zijn. Weegt het belang van honderd procent zekerheid op tegen de offers (privacy, kosten, moeite) die de burger zich moet getroosten?

3. De regie: publiek versus privaat

Wie moet het initiatief en de regie rond de vormgeving van digitale identificatie op zich nemen? Waar en onder welke omstandigheden moet de overheid een monopolie hebben en waar mag (of zelfs moet) ze ruimte laten voor marktpartijen? Voor welke sectoren? Wie zetten de standaards? Waar moet de overheid handelen en waar juist niet?

4. De wens: gemak en resultaat versus vrijheid

De ontwikkelingen op het gebied van de informatie- en communicatie-technologie hebben ons maatschappelijk en sociaal functioneren de afgelopen jaren in vele opzichten eenvoudiger gemaakt. Ook de publieke sector heeft haar voordeel kunnen doen met ICT. De consequentie van deze ontwikkelingen kan zijn dat de overheid de beschikking krijgt – of denkt te hebben – over een vrijwel compleet beeld van het doen en laten van haar burgers. Vanuit de veronderstelling dat al deze informatie ook de juiste informatie is, biedt de overheid met deze vergaande vorm van identificatie de garantie dat procedures efficiënter en sneller kunnen worden afgehandeld. Maar het is de vraag hoever de burger optimalisatie onder het mom van ‘gemak’ accepteert. Waar trekt de overheid de grens en waar laat ze het initiatief en de regie over aan de burger?

Aanbevelingen

De genoemde kwesties zijn complex en de te maken keuzes onderling sterk gerelateerd. Niettemin biedt deze publicatie een aantal aanbevelingen voor het toekomstige overheidsbeleid rond digitale identificatie. Stilzitten is immers geen optie, want dat leidt op macro-niveau tot maatschappelijk en economisch verlies.

- 1. De overheid doet er goed aan meer onderzoek te laten verrichten naar de burgerbeleving van digitale identificatie. De belangen van burgers zijn in de discussie op dit moment nog onderbelicht.*
- 2. Daarnaast moet zij een sectoroverschrijdend, integrerend debat initiëren en vormgeven. Vier punten zijn van belang bij de vormgeving van dat debat:*
 - langetermijnontwikkelingen moeten leidend zijn;*
 - het debat moet zich losmaken van de focus op identificatiemiddelen;*
 - het debat moet open zijn, ofwel niet in achterkamers worden gevoerd;*
 - het debat moet leiden tot een breed gedragen beleidsvisie die aanzet tot handelen*

Verder is het volgende nodig:

- 1. Het scheppen van een stelsel brengt tal van kwetsbaarheden met zich mee. Daarom zullen er checks and balances nodig zijn: een soort digitaal voorzichtigheidsbeginsel, gekoppeld aan een hoge mate van juridische precisie.*
- 2. Daarnaast bestaat behoefte aan een structuur voor coördinatie: de belangentegenstellingen zijn groot en er zit een scala aan deelnemers aan de beleidstafel.*
- 3. Hoewel het scheppen en beheren van een digitaal identificatiestelsel een collectief goed is, is een vorm van publiek-private samenwerking op dit terrein zeker niet ondenkbaar. Dan zal wel moeten worden gezien waar men door samenwerking van elkaar kan leren, waar de overheid het bedrijfsleven de vrije teugel kan geven en waar de overheid de regie moet houden.*

1 Inleiding

1.1 Digitale identificatie boeit

The Net is een beklemmende film. Hoofdpersoon Angela Bennett, een telewerkende *computernerd* zonder vrienden of familie (alleen een moeder met Alzheimer), wordt door een bende slechteriken ontdaan van haar fysieke identiteitsbewijzen. Bovendien worden al haar computerwachtwoorden, toegangscode, bankrekeningen en pincodes geblokkeerd. Met behulp van de computer wordt haar hele administratieve bestaan uitgewist. Gaandeweg de film wordt duidelijk dat het ontbreken van haar digitale identiteit en haar onmacht om zich te identificeren het voor Bennett onmogelijk maken om nog op enige manier te functioneren: de facto heeft zij opgehouden te bestaan.

Bij *identificatie* van personen draait alles om het kunnen koppelen van bepaalde informatie aan een bepaalde identiteit, aan de 'afbeelding' die van een bepaald persoon bestaat. Deze publicatie beperkt zich uitsluitend tot de identificatie van personen, niet tot de identificatie van objecten. Aldus kan worden vastgesteld of de door een persoon gebruikte identiteit ook werkelijk bij hem of haar hoort. Dit wil niet zeggen dat daarmee per se is vastgesteld dat het daadwerkelijk om die ene persoon gaat, maar wel dat de persoon in kwestie al dan niet bevoegd is om een bepaalde handeling te verrichten.

De film *The Net* maakt op indringende wijze duidelijk dat de mogelijkheid om iemand succesvol te kunnen identificeren tot de meest waardevolle zaken van onze samenleving behoort. In het dagelijks leven doen zich talrijke contacten voor tussen particulieren, bedrijven en overheid waarvoor een vorm van identificatie nodig is. Identificatie staat bijvoorbeeld aan de basis van overheidsdienstverlening aan individuen (zoals het verlenen van een bouwvergunning) en inkomensoverdrachten (bijvoorbeeld het betalen van belasting en het verkrijgen van een uitkering). Om democratische rechten uit te voeren (de organisatie van verkiezingen en voldoen aan informatieplichten) is het essentieel dat de overheid weet met wie ze van doen heeft. Daarnaast vormt identificatie het draaipunt bij uitstrek om de openbare orde te handhaven en de veiligheid te vergroten.

In veel opzichten vormt identificatie het smeermiddel dat maatschappelijk functioneren mogelijk maakt. Om het hele proces soepel te laten verlopen, heeft de overheid een identificatiestelsel geschapen. Binnen dit stelsel spelen fysieke identificatiemiddelen (vooral papieren identiteitsdocumenten) een belangrijke rol. Deze identificatiemiddelen zijn dragers van identiteitsinformatie die (al dan niet direct)

ontleend is aan de geboortekte. Dit geldt vaak ook voor identificatiemiddelen die de private sector uitgeeft.

Hoewel de emoties soms hoog kunnen oplopen tijdens discussies over de invoering van een algemene identificatieplicht, was het bestaande stelsel van identificatie tot voor kort geen onderwerp waarover men zich echt zorgen hoefde te maken. Meerdere stelsels van regels, instituties en ondersteunende informatiesystemen creëerden betrouwbare identificatiemiddelen, waarmee de koppeling tussen informatie en identiteit vrijwel probleemloos gemaakt kon worden. Onze samenleving is echter fundamenteel aan het veranderen: informatisering, globalisering, horizontalisering van verhoudingen en ontwikkelingen op het gebied van informatie- en communicatietechnologie (ICT) zijn daarin drijvende krachten en elkaar wederzijds beïnvloedende katalysatoren. Internet is de meest manifeste illustratie van dit proces. Steeds meer transacties vinden plaats via dit medium. Internet neemt echter het aloude *face-to-face*-contact weg. Ook werken hier oude methoden om iemands identiteit te controleren niet langer. De automatisering van de samenleving vraagt dus om digitale equivalenten van de fysieke vormen en middelen van identificatie. Zonder een goed functionerend stelsel van digitale identificatie zal bijvoorbeeld de criminaliteitsbestrijding (zowel binnen als buiten *cyberspace*) ernstig bemoeilijkt worden, zullen ambities op het gebied van *e-government* gefrustreerd worden, zullen bedrijven en burgers vertrouwen missen in *e-commerce*-activiteiten en zal uiteindelijk onze (beleids)concurrentiepositie verslechteren. Het is daarom noodzakelijk om na te denken over de vormgeving van een goed functionerend digitaal identificatiestelsel.

Tot op heden zijn de ontwikkelingen op het terrein van digitale identificatie vooral sectoraal en functioneel ingekleurd: tal van procedures en passen met persoonlijke codes zijn ontwikkeld om met digitale technieken in een vastomlijnde en contextgebonden situatie een bepaald kenmerk aan een bepaalde persoon te hangen. Te denken valt aan initiatieven als de Zorgpas en thuisbankieren. Tegelijkertijd zijn sectoroverstijgende initiatieven zichtbaar: zo wordt nagedacht over de toepassing van biometrie in onze identiteitsbewijzen en doet zelfs de Europese Commissie enkele voorzichtige schreden op het pad dat (wellicht) moet leiden tot een Europees stelsel van digitale identificatiemiddelen. Aldus zijn diverse gremia bezig met (deelaspecten van) digitale identificatie. Vanaf een afstand bezien, ontstaat echter de indruk dat deze initiatieven veelal sterk geïsoleerd en verkokerd zijn. Bovendien lijkt er soms ook sprake van een Babylonische spraakverwarring: de verschillende initiatieven hanteren niet dezelfde uitgangspunten en definities voor begrippen als identiteit, identificatie en identificatiemiddel. Dit leidt er niet alleen toe dat de betrokken partijen elkaar soms niet verstaan, ook kunnen natuurlijke dwarsverbanden verborgen blijven.

1.2 Doel van de publicatie

We staan aan de vooravond van enkele fundamentele beslissingen omtrent de creatie van een stelsel van digitale identificatie. Tegen die achtergrond wil deze publicatie de leden van het parlement in staat stellen zich een beter beeld te vormen van de:

- problematiek rondom digitale identificatie;
- relevante beleidsinitiatieven, hun context en doelstellingen, mede in het licht van huidige politieke ambities;
- keuzes waarvoor we staan en de mogelijke ontwikkelingsrichtingen die zich aftekenen.

Deze publicatie beoogt een praktisch hulpmiddel te zijn bij het inlezen in het onderwerp, zodat parlementariërs en andere geïnteresseerden snel en gemakkelijk een overzicht van en inzicht in de materie en belangen krijgen, en zich ervan bewust worden welke keuzes gemaakt moeten worden en de consequenties die deze kunnen hebben. Kortom: de publicatie informeert, problematiseert en politiseert.

1.3 Opzet

De publicatie bestaat uit drie hoofdstukken. Na de inleiding geeft hoofdstuk 2 aan de hand van vier thema's een overzicht van de belangrijkste ontwikkelingen in Nederland en Europa, die voor de komende jaren relevant zijn. Daarmee laat het hoofdstuk zien dat, ondanks het caleidoscopische en complexe karakter van de materie, ook een aantal gemeenschappelijke ontwikkelingen te ontwaren zijn. Aan de hand daarvan presenteert hoofdstuk 3 de fundamentele keuzes waarvoor we staan, evenals de mogelijke (toekomstige) implicaties van deze keuzes. Tot slot biedt het een aantal handreikingen voor de verdere discussie over digitale identificatie.

1.4 Methodiek

De hoofdstukken 1 en 2 zijn geschreven op basis van uitgebreide desk-research, waarbij beleidsstukken en publicaties van de afgelopen twee jaar bestudeerd zijn. Het laatste hoofdstuk is gebaseerd op kennis en meningen van personen die betrokken zijn bij (het denken over) de vormgeving van het beleid. Deze informatie is ontleend aan diepte-interviews en een workshop die het Rathenau Instituut organiseerde op 13 mei 2002 in Den Haag (zie bijlage 2).

2 Overzicht van beleidsinitiatieven rond digitale identificatie

2.1 Inleiding

Om te kunnen bepalen welke kant het op moet met digitale identificatie, zal eerst moeten worden vastgesteld waar we op dit moment staan. Zowel uit de interviews als uit de workshop die georganiseerd is in het kader van deze publicatie (zie bijlage 1 en 2) blijkt dat in het veld een totaaloverzicht ontbreekt. Daarom onderneemt dit hoofdstuk een poging om een beeld te scheppen van wat er op nationaal en Europees niveau zoal speelt op het gebied van digitale identificatie.

Als insteek is gekozen voor het clusteren van de bestaande initiatieven rond enkele thema's die naar verwachting in de huidige maatschappelijke context actueel zullen blijven (zie bijlage 3). Na de val van het kabinet-Balkenende in oktober 2002, hebben CDA en VVD laten weten dat de hoofddoelstellingen uit het Strategisch Akkoord onverminderd van kracht zullen blijven tot de nieuwe verkiezingen van 2003. Indien de coalitie tussen beide partijen na de verkiezingen wordt doorgezet, zullen deze doelstellingen relevant blijven. Daarmee zien we dat twee thema's pregnant op de beleidsagenda staan: (1) veiligheid (vooral de bestrijding van criminaliteit en fraude) en (2) vreemdelingenbeleid. Vanuit een Europees perspectief zal ook elektronische dienstverlening hoog op de agenda staan. Dit wordt verder ingegeven door de noodzaak tot bezuinigen en door autonome, deels onomkeerbare ontwikkelingen vanuit de informatisering in de private sector en de lokale overheid. Deze 'e-dienstverleningsthema's' zijn: (3) dienstverlening door de overheid en (4) efficiency van de overheid.

Voordat het overzicht van de beleidsinitiatieven in relatie tot de genoemde thema's in paragraaf 2.3 wordt gegeven, gaan we eerst kort in op het verband tussen de thema's en digitale identificatie. Vervolgens schetst paragraaf 2.4 een aantal gemeenschappelijke initiatieven. Dit hoofdstuk wordt afgesloten met enkele conclusies.

2.2 Digitale identificatie en vier relevante beleidsthema's voor de toekomst

Digitale identificatie is vaak een belangrijk aangrijpingspunt bij het voorgenomen beleid op de bovengenoemde thema's. Dikwijls is het zelfs een onmisbare schakel of zelfs een wezenlijk instrument bij het realiseren van het beleid.

2.2.1 Veiligheid

Digitale identificatie speelt een belangrijke rol op het gebied van veiligheid. De virtualisering van onze samenleving maakt het mogelijk praktisch anoniem, dan wel met een vervalste of gestolen identiteit, strafbare handelingen te verrichten. Tegelijkertijd zien we dat de grenzen van opsporingsbevoegdheden, die in de niet-virtuele wereld redelijk vastlagen, plotseling verschuiven in het nadeel van de verdachte: de politie maakt tegenwoordig gebruik van technische mogelijkheden waarvan het vaak niet duidelijk is of die de toets met de rechtmatigheid wel kunnen doorstaan. Hierbij valt te denken aan de praktijk om elektronische berichten af te tappen, maar ook aan een recent geval waarbij de politie vanuit een helikopter met warmtezoekende apparatuur hennepkwekerijen opspoorde. Het (vermeende) algehele gevoel van onveiligheid dat is ontstaan na de terroristische aanslagen van 11 september 2001, zet daarbij de toon. Bij het plegen, opsporen en bestraffen van strafbare feiten is het essentieel dat de daad kan worden gekoppeld aan de dader, binnen de daarvoor geschapen wettelijke kaders. Identificatie vormt daarbij het draaipunt, zowel in de fysieke als in de virtuele wereld.

Binnen deze context zet het regeerakkoord stevig in op criminaliteitsbestrijding en rechtshandhaving: deze moeten doeltreffender worden door de invoering van een algemene identificatieplicht, een ruimere toepassing van DNA-technieken en cameratoezicht op plaatsen met een verhoogd risico op criminaliteit. Verder moet de samenwerking met en informatie-uitwisseling tussen politie, marechaussee, douane, Openbaar Ministerie, reclassering, voogdij-instellingen en andere instellingen worden verbeterd. Zo wil de regering een doelmatige bestrijding bevorderen, overlappende werkzaamheden voorkomen en een tijdige signalering mogelijk maken om, waar nodig, personen te kunnen volgen. De mogelijke consequenties voor en de belangen van de rechten van de verdachte komen niet specifiek aan de orde in het regeerakkoord.

2.2.2 Vreemdelingenbeleid

Een tweede belangrijk beleidsthema is het vreemdelingenbeleid. Het regeerakkoord van het kabinet-Balkenende I meldde dat de komende jaren een restrictief vreemdelingenbeleid gevoerd zou worden en illegaal verblijf met kracht zou worden bestreden. Ook onder een nieuwe regering zal dit onderwerp van groot politiek belang blijven. Er is een zeer directe koppeling tussen vreemdelingenbeleid en digitale identificatie. Juist in deze sector zien we dat een *track record* ontbreekt: het komt dikwijls voor dat asielzoekers geen identiteitspapieren bij zich hebben, terwijl er evenmin geput kan worden uit gegevens waarmee de identiteit kan worden vastgesteld. Niettemin is er grote behoefte om een identiteit vast te stellen of toe te kennen tijdens de periode dat de vreemdeling in Nederland verblijft. We zien dan ook dat in deze sector al veel gebruik wordt gemaakt van biometrische technieken waarmee de overheid een unieke koppeling kan leggen tussen persoonskenmerken en een persoon. Bovendien tekenen zich contouren af van Europese samenwerking op dit vlak, waarbij (biometrische) gegevens worden uitgewisseld tussen de lidstaten.

2.2.3 Dienstverlening door de overheid

Zonder digitale identificatie is overheidsdienstverlening op afstand niet mogelijk. Internet, als materialisatie van de netwerksamenleving, neemt een steeds belangrijker plaats in ons leven in: steeds meer contacten en transacties vinden plaats via dit medium. Internet neemt echter het *face-to-face* contact weg en oude mogelijkheden tot verificatie van een identiteit – zoals het controleren van een paspoort – werken niet langer. Wil *e-government* een einde maken aan de fase van ‘omgevallen folderkast’, dan is het van vitaal belang dat er een mechanisme wordt geschapen waarbij de overheid – maar ook het bedrijfsleven – er zeker van kan zijn dat zij met het individu te maken heeft waarmee ze denken van doen te hebben. Dit is vooral belangrijk omdat de rechtsgevolgen van een transactie met de overheid (zoals een vergunning of een bepaalde status verwerven) vaak veel verstrekkender zijn dan een transactie in de private sector. Daar komt nog bij dat een betrouwbare identiteitsinfrastructuur essentieel is voor de interferentie tussen *e-commerce* en *e-government*.

In het regeerakkoord van het kabinet-Balkenende I komt dienstverlening door de overheid er bekaaid vanaf. Het kabinet had zich voorgenomen door minder regelzucht en bureaucratie meer ruimte te scheppen voor eigen keuzen van de burger, maar de initiatieven die tijdens Paars II vooral door minister R.H.L.M van Boxtel op dit gebied zijn geïnitieerd worden niet genoemd. Toch zullen de onder het tweede kabinet-Kok in gang gezette ontwikkelingen niet op een dood spoor eindigen. Allereerst is daar natuurlijk de huidige noodzaak om bezuinigingen door te voeren. ICT kan daarbij een belangrijk middel zijn, omdat het efficiency-

verbetering mogelijk maakt. Maar ook vanuit andere hoeken stellen we vast dat dit thema nog steeds hoog op de agenda staat. In de eerste plaats zien we dat vanuit Brussel zeer fors ingezet wordt op *e-government*. Zowel het nieuwe *eEurope Action Plan* (en het daarmee samenhangende *e-government Action Plan 2002-2005*) als het zesde Kaderprogramma reserveert substantiële bedragen voor initiatieven op dit gebied, nog afgezien van het *commitment* dat is aangegaan onder andere Europese programma's (IDA II, eContent et cetera).

Naast deze Brusselse initiatieven is er in Nederland op decentraal bestuurlijk niveau een aantal ontwikkelingen in gang gezet die een geheel eigen dynamiek hebben gekregen: iedere zichzelf respecterende gemeente is inmiddels op internet te vinden en op grote schaal vinden experimenten plaats met dienstverlening (en daarbij behorende digitale identificatie). Dit is een onomkeerbaar proces.

2.2.4 Efficiency van de overheid

Niet alleen aan de voorkant van het overheidsbedrijf speelt digitale identificatie een rol; ook in de *backoffice* zal digitale identificatie gebruikt (kunnen) worden om processen binnen de overheid doelmatiger te laten verlopen. Hierbij valt vooral te denken aan de initiatieven voor stroomlijning van onderlinge gegevensuitwisseling of aan de plannen om gegevens die diverse overheden thans telkens weer opnieuw bij burgers en bedrijven opvragen, slechts eenmalig te verstrekken en zo hergebruik te verplichten.

Het Strategisch Akkoord van het kabinet-Balkenende stelde in dit kader dat het bestuur de laatste jaren weliswaar dichterbij de burger is gebracht, maar dat dit juist het oplossend vermogen van de overheid heeft doen afnemen en de onvrede bij burgers heeft doen toenemen. Daarom wilde het kabinet komen tot verdergaande stroomlijning van procedures om zo de daadkracht en besluitvaardigheid van de overheid te vergroten. Als voorbeeld wordt genoemd de te leggen koppeling tussen de Wet Onroerende Zaakbelasting (WOZ) en de Gemeentelijke Basisadministratie Persoonsgegevens (GBA). ICT moet daarbij een belangrijke rol spelen.

2.3 De beleidsthema's van de toekomst in relatie tot de initiatieven van nu

Het voorgaande laat zien dat digitale identificatie, al meeliftend op de rug van de vier beleidsthema's, in instrumentele zin duidelijk op de beleidsagenda voor de komende periode staat. De regering die in 2003 aantreedt, zal naar verwachting deze koers voortzetten. Wel valt op dat de insteek is veranderd: werd onder Paars II vooral gekeken

naar de rol van digitale identificatie bij de overheidsdienstverlening, thans ligt de nadruk meer op de rol die zij kan spelen bij een effectiever beleid op het terrein van criminaliteitsbestrijding, veiligheid en vreemdelingenbeleid. De vraag rijst dan welke consequenties deze koerswijziging heeft voor reeds in gang gezette initiatieven waarbij digitale identificatie (en vooral digitale identificatiemiddelen) een rol speelt. Sluiten de toekomstplannen aan bij eerdere projecten of wijken ze daar (in al dan niet belangrijke mate) van af?

Ten eerste valt op dat het perspectief thans zeer eenzijdig is geworden: de discussie wordt vooral gevoerd vanwege het belang voor de thema's veiligheid en vreemdelingenbeleid. De consequentie is dat deze brandende thema's nauwelijks lijken aan te sluiten bij de lopende programma's en projecten. Werd tijdens de paarse kabinetten vooral ingezet op infrastructurele voorzieningen voor digitale identificatie (stroomlijning basisgegevens, herziening van de Gemeentelijke Basisadministratie Persoonsgegevens, GBA). In de afgelopen periode kregen deze onderwerpen met het oog op een betere dienstverlening en een efficiëntere uitvoeringsorganisatie nauwelijks of geen aandacht.

Ook op Europees niveau mogen we verwachten dat digitale identificatie in relatie tot veiligheid belangrijker gaat worden. Momenteel zijn de (regelgevings)initiatieven die iets met digitale identificatie van doen hebben, nog vooral georiënteerd op het (privaatrechtelijke) handelsverkeer of hebben een tamelijk praktische insteek, zoals de digitale tachograaf en het delen van informatie (Schengen). Blijkens de enquête die begin 2002 onder Spaans voorzitterschap onder de lidstaten werd gehouden, zal deze marginale en vanuit interne marktoptiek gedreven aanpak niet eeuwig duren. In die enquête werd de lidstaten gevraagd in hoeverre de Europese Commissie een actieve rol zou kunnen spelen op het gebied van digitale identiteitsmanagement. Het is, gezien het gedrag van de Europese Commissie op andere terreinen, niet denkbeeldig dat de Commissie activiteiten zal gaan ontwikkelen op het terrein van digitale identificatie en veiligheid. Vreemdelingenproblematiek en de bestrijding van terrorisme zijn, politiek gezien, uitstekende aanleghavens. Ondanks de verwachte groei van Europese bemoeienis met digitale identificatie zal de meerderheid van de beleidsvoornemens voorsnog vanuit nationaal niveau worden ontwikkeld. Immers, de bevoegdheid daartoe ontbreekt voorsnog grotendeels: de genoemde beleidsgebieden zitten nog steeds in de competentiesfeer van de lidstaten.

De nationale voedingsbodem voor initiatieven rondom digitale identificatie zal naar verwachting wel een andere samenstelling hebben dan voorheen. Gezien het economisch tij – in combinatie met de nieuwe beleidsprioriteiten – valt te vrezen dat enkele ontwikkelingen die in het verleden in gang zijn gezet, geen stand zullen houden in de voorgenomen bezuinigingsoperatie. Op sommige gebieden deert dat niet,

omdat het beleid reeds gekiemd is en de voortgang redelijk onafhankelijk is van ondersteuning door de centrale overheid. Een voorbeeld hiervan is de elektronische dienstverlening op gemeentelijk niveau. De lopende initiatieven die binnen de speerpunten van het nieuwe beleid passen, zullen naar verwachting ook doorgaan – denk bijvoorbeeld aan de asielpas en de verdere ontwikkeling van identificatiemiddelen met biometrische kenmerken.

Andere initiatieven zullen het echter hoogstwaarschijnlijk niet kunnen stellen zonder een verdere impuls en stevige ondersteuning. Het gaat daarbij vooral om voorzieningen die niet direct onder de hoede van één ministerie vallen, maar juist door hun collectieve karakter op afstand zijn gezet en gedragen worden door meerdere ministeries. Een voorbeeld zijn de diverse programma's (zoals het programma Stroomlijning Basisgegevens) die zijn ondergebracht bij ICTU. Deze organisatie voert projecten uit, waarbij samenwerking op ICT-gebied tussen overheidsorganisaties centraal staat. Daarbij beweegt ICTU zich tussen beleidsontwikkeling en uitvoering (zie www.ictu.nl). Juist deze programma's willen de broodnodige informatiele infrastructuur scheppen, zoals het scheppen van een stelsel van authentieke registraties. Nu dit programma Stroomlijning Basisgegevens is gestopt, is het maar de vraag of onderdelen daarvan (bijvoorbeeld het project gericht op het scheppen van een authentieke basisregistratie voor adressen) al ver genoeg zijn gevorderd om op eigen benen te staan.

Gegeven de te verwachten beleidswijziging, treedt de vraag naar voren wat de implicaties hiervan zullen zijn voor de fundamentele vragen die spelen bij de discussie over de totstandbrenging van een stelsel van digitale identiteiten en systemen voor digitale identificatie. Uit het navolgende overzicht van lopende beleidsinitiatieven en uit de analyse daarvan, zal blijken dat de koerswijziging in beleid in feite nauwelijks van invloed zal zijn op een aantal duidelijke trends, gemeenschappelijkheden en opmerkelijkheden die zichtbaar zijn.

2.4 Schematisch overzicht van de initiatieven rond digitale identificatie

Dit schema geeft aan op welke thema's de initiatieven spelen die ontwikkeld worden rond, dan wel een impact hebben op digitale identificatie.¹ Voorts bevat het schema een korte omschrijving van het soort initiatief en geeft het aan wie de initiatiefnemer is.

Schema digitale initiatieven

Initiatieven	Thema's				Initiatiefnemer	Soort initiatief
	Veiligheid	Vreemdelingenbeleid	Dienstverlening	Efficiency		
Europese initiatieven						
Richtlijn elektronische handel			X		Europese Unie	Regelgeving
Richtlijn elektronische handtekening			X		Europese Unie	Regelgeving
Schengen Informatie Systeem	X				Europese Unie	Delen van informatie
Europese gezondheidskaart			X	X	Europese Unie	Delen van informatie
Eurodac	X	X			Europese Unie	Delen van informatie
Digitale tachograaf	X				Europese Unie	Technische samenwerking
Europese raadpleging digitale identiteit	-	-	-	-	Europese Unie	Beleidsvoorbereidend initiatief
Nederlandse initiatieven						
Haalbaarheidsstudie elektronische identiteitskaart	X	X			BZK	Infrastructurele maatregelen
Haalbaarheidsstudie biometrie in reisdocumenten	X	X			BZK	Infrastructurele maatregelen
De nieuwe generatie reisdocumenten	X	X			BZK	Infrastructurele maatregelen
De modernisering van de GBA			X	X	BZK	Infrastructurele maatregelen
Digitaal kluisje			X	X	BZK	Infrastructurele maatregelen
Stroomlijning basisgegevens			X	X	BZK/ICTU	Infrastructurele maatregelen
Advies van de Tafel 'Persoonsnummerbeleid in het kader van identiteitsmanagement'	X		X	X	BZK/ICTU	Beleidsvoorbereidend initiatief (infrastructuur, regelgeving)
PKIoverheid	X		X	X	BZK	Infrastructurele maatregelen
Onderwijsnummer				X	OCenW	Infrastructurele maatregelen, ondersteund met regelgeving

Initiatieven	Thema's				Initiatiefnemer	Soort initiatief
	Veiligheid	Vreemdelingenbeleid	Dienstverlening	Efficiency		
Cliënt-volg-communicatiestelsel			X	X	SZW	Delen van informatie
RINIS				X	SZW	Delen van informatie
Taskforce sofi-fraude	X				SZW en Financiën	Beleidsvoorbereidend initiatief
Elektronisch patiëntendossier (EPD)			X	X	Volksgezondheid	Delen van informatie
Registratie van probleemjongeren	X			X	BZK	Delen van informatie
Verwijsindex personen (VIP)	X			X	Justitie	Delen van informatie
Parkinson-pas			X	X	Volksgezondheid	Chipcard
OV-kaart			X	X	VenW	Chipcard
Chauffeurspas voor taxichauffeurs				X	VenW	Chipcard
(1) Vreemdelingenkaart en (2) Asielpas		X			Justitie	Chipcard en informatie delen
Previumpas Schiphol	X		X	X	N.V. Schiphol in samenwerking met private sector	Chipcard
Defensiekaart	X		X	X	Defensie	Chipcard
Multifunctionele studentenchipkaart			X	X	OCenW	Chipcard
Negatief basisregister paspoorten gecombineerd met aanpassing paspoortwet	X				BZK	Regelgeving en delen van informatie
Wettelijke identificatieplicht	X	X			Justitie	Regelgeving
Implementatie Vreemdelingenwet 2000		X			Justitie	(Uitvoering van) regelgeving
Wet DNA	X				Justitie	Regelgeving
Overheidsloket 2000			X		BZK/ICTU	Faciliterende maatregelen
Elektronisch autokenteken				X	VenW	Technische maatregelen
Rijbewijs	X				VenW	Regelgeving
65+-pas			X		Volksgezondheid	Faciliterende maatregelen

2.5 Analyse van de initiatieven

Wanneer we de in het bovenstaande schema genoemde beleidsinitiatieven analyseren, worden acht ontwikkelingen zichtbaar.

2.5.1 Spraakverwarring

In de eerste plaats valt op dat een eenduidige semantiek ontbreekt: beleidsstukken maken veelal geen – en als zij dit wel doen, niet eenduidig – onderscheid tussen het *concept* identiteit, het *proces* van identificatie en het *middel* dat daarbij wordt gebruikt (zie ook bijlage 1). Een eenduidig begrippenapparaat is echter een eerste voorwaarde voor het startpunt van een doortimmerde politieke, wetenschappelijke en maatschappelijke discussie over een stelsel van betrouwbare identiteiten en systemen van digitale identificatie.

2.5.2 Overconcentratie op middelen

De huidige discussie blijft veelal beperkt tot de inzet van nieuwe identificatiemethoden en de mate waarin middelen als nummers, codes, chipkaarten, biometrie en DNA daarvoor moeten en mogen worden ingezet. In het verlengde van deze discussie komen soms vragen naar voren die niet zozeer over het gebruikte middel gaan, maar over het *niveau* van identificatie: willen we in alle situaties burgers kunnen identificeren (iemand's ware identiteit vaststellen), of kunnen we soms ook volstaan met verificatie (behoren de getoonde gegevens werkelijk bij de persoon die we voor ons hebben)?

2.5.3 Smartcards: beperkt succes en niet geïntegreerd

De voorspelling van eind jaren negentig dat de zogeheten smartcards overall in het openbaar bestuur als identificatiemiddel gebruikt zouden gaan worden, is niet uitgekomen (Thaens, Zouridis & Kielema 2002 o.c., pp.19-20). Hoewel een groot aantal experimenten is opgezet, zijn vele een zachte dood gestorven; andere zijn veel later dan gepland van start gegaan en dikwijls in afgeslankte vorm. Veel projecten hebben bovendien niet gebracht wat er van verwacht werd. De multifunctionele burgerservicekaart is een voorbeeld hiervan. De burgerservicekaart zou, naast een door biometrie ondersteund elektronisch identificatiemiddel, ook andere functionaliteiten herbergen, zoals parkeervergunningen, bibliotheeklidmaatschap, et cetera. De kaart zou een publiek en een privaat deel bevatten, waardoor het mogelijk zou worden om ook allerlei commerciële toepassingen op de burgerservicekaart te plaatsen. Afgezien van een experiment in Haarlem, is er echter weinig van terechtgekomen.

Inmiddels heeft het agentschap BPR (Basisadministratie Persoonsgegevens en Reisdocumenten) zich uitgesproken tegen het gebruik van een kaart voor meerdere doelen, zoals met de burgerservicekaart beoogd werd. Het uitgangspunt voor de nieuwe generatie reis- en identificatiedocumenten is daarom dat ook eventuele smartcards alleen voor dit specifieke doel gebruikt kunnen worden. Waar toch grote experimenten worden opgestart, worden relatief eenvoudige en duidelijk afgebakende terreinen betreden. Zo is de Zorgpas – een initiatief waarbij patiënten- en consumentenorganisaties, verzekeraars en zorgaanbieders betrokken zijn – een relatief ‘domme’ kaart. Op de Zorgpas kunnen slechts in beperkte mate gegevens worden bijgeschreven of veranderd.

2.5.4 Toenemend gebruik van biometrie

Met behulp van biometrische technieken is het mogelijk unieke lichamelijke kenmerken aan een persoon te koppelen en hem op deze wijze te identificeren. Zo wordt gebruikgemaakt van biometrie bij vingerafdrukherkenning, handgeometrieherkenning, irisscan, retinascan en herkenning van het warmtepatroon van het gelaat. Ook gedragskenmerken, zoals de manier van lopen, stemgeluid en dynamische handtekeningen kunnen worden gebruikt. Steeds meer initiatieven maken gebruik van biometrie. Zo kunnen asielzoekers in Rotterdam op deze manier bij de politie aan hun periodieke meldingsplicht voldoen. In Delft is men bezig met het scannen van vingertoppen en in Hilversum loopt een proef met identificatie door middel van gezichtsherkenning. Door biometrische gegevens te verwerken in identificatiemiddelen, kunnen deze fraudebestendiger gemaakt worden: zo kunnen dubbelgangers minder makkelijk elkaars paspoort gebruiken. Met deze techniek kunnen ook burgers zich met behulp van hun unieke lichaamskenmerken ‘op afstand’ identificeren – via bijvoorbeeld internet of in openbare gelegenheden geplaatste informatiezuilen – en zo toegang hebben tot elektronische voorzieningen van de overheid. De identificatie kan ook thuis gebeuren: direct nadat de computer wordt aangezet, scant een camera bijvoorbeeld de ogen van de gebruiker. Unieke kenmerken van de iris zijn gekoppeld aan een persoonlijke inlogcode, die weer is gekoppeld aan een bankrekeningnummer of stembiljet (cf. ‘Biometrische handtekening’ 2001). Voormalig minister Van Boxtel was een vurig voorstander van biometrie en ook nu nog bestaat het voornemen om bij de vervaardiging van het digitale paspoort biometrie te gebruiken.

2.5.5 Gebruik van nummers neemt toe

Niet alleen de inzet van biometrie is populair. Nummers fungeren traditioneel als identificerend kenmerk voor personen. Immers, nummers zijn bij uitstek handig om een unieke koppeling aan te brengen en grote bestanden aan te leggen. Met nummers kun je makkelijk reke-

nen en oneindig variëren. Uit onderzoek blijkt dat ruim zeventig procent van alle grote overheidsregistraties gebruikmaakt van een administratienummer en het gebruik van landelijke identificatienummers significant stijgt. Naast het A-nummer en het Fi- of sofi-nummer worden onder meer het kadastraal nummer, het militair registratienummer en het onroerend goednummer landelijk gebruikt.²

2.5.6 Meerketengebruik van nummers

Behalve het toenemend gebruik van nummers, lijken ze ook te worden 'ontketend'. We zien vooral bij uitvoeringsinstanties en de sterk geautomatiseerde fiscale en sociale zekerheidssectoren een groeiende behoefte aan integratie van de verschillende landelijk gebruikte nummers.

Het sofi-nummer is daarvan het beste voorbeeld. Het heeft zich door toenemend intersectoraal gebruik in een kleine twintig jaar ontwikkeld van een geheim intern nummer tot een quasi algemeen verplicht persoonsnummer (meerketengebruik) (Grijpink 2002). Zo wordt het onder meer gebruikt in de sociale sector (als koppelingsnummer), in de onderwijssector en zal het in de toekomst waarschijnlijk in de zorgsector de functie krijgen van zorgidentificatienummer (ZIN), ofschoon dit laatste niet onomstreden is.³ Voorts staat het nummer in het paspoort en het rijbewijs,⁴ waardoor allerlei instanties binnen en buiten de overheid het nummer rechtmatig van een getoond identiteitsbewijs kunnen overnemen en (intern) kunnen gebruiken. Saillant is ook dat (gerechts)deurwaarders voor de uitvoering van hun bij wet opgedragen publiekrechtelijke taak bij het leggen van executoriaal beslag onder derden, de bevoegdheid hebben gekregen voor het gebruik van het sofi-nummer.

Om in deze behoefte aan geïntegreerd nummergebruik te voorzien, komt het ministerie van Binnenlandse Zaken nu met plannen om een Burger Service Nummer te introduceren. Iedere Nederlander moet in de toekomst één nummer krijgen, waarmee hij zich in al zijn contacten met overheidsinstanties kan identificeren. Niet alleen moet dit nummer het voor de burger eenvoudiger maken om toegang te krijgen tot overheidsdiensten, tegelijkertijd moet het de dienstverlening efficiënter en transparanter maken.

2.5.7 Monopolie van de overheid bij de toekenning van identificatiemiddelen wankelt

Vanaf het moment dat een ouder de geboorte van een kind bij de gemeente aangeeft, is de bevolkingsadministratie de meest centrale en doorslaggevende bron voor onze identiteitsvaststelling. Vele andere bronnen zijn een afgeleide van de bevolkingsadministratie, of zij ontleen aan deze administratie de informatie die ze nodig hebben om te kunnen fungeren als een identiteitsbron. Ook bij de toekenning van

digitale identificatiemiddelen is de publieke sector vooralsnog de meest vooraanstaande bron. De particuliere afgeleiden van publieke identiteitsbronnen zijn veelal beperkt in tijd, functie en reikwijdte van het gebruik (zoals bankpasjes, abonnementen, jaar kaarten).

Toch lijkt hierin verandering te komen. De opkomst van digitale technieken maakt het voor de private sector namelijk steeds eenvoudiger en vanzelfsprekender om instrumenten te ontwikkelen die kunnen worden ingezet voor de identificatie en verificatie van personen. Deze instrumenten zijn lang niet altijd afgeleid van of gebaseerd op publieke identiteitsbronnen. In de virtuele, grenzeloze wereld van internet ontstaan bijvoorbeeld identificatiemiddelen die zelfs geheel losstaan van hun op publieke bronnen gebaseerde *offline* tegenhangers. Sommige ondernemingen (zoals Microsoft met zijn Passport) lijken inmiddels een belangrijke positie te verwerven op de digitale identiteitsmarkt. Indien de overheid zich niet (voldoende) bemoeit met het opzetten van een systeem van digitale identificatie, is het denkbaar dat het bedrijfsleven de toon gaat zetten en de (technische) voorwaarden zal dicteren. Dat zou kunnen betekenen dat ook de overheid voor haar elektronische dienstverlening gebruik zal moeten maken van door de markt ontwikkelde en tot standaard verheven identificatie-instrumenten.

2.5.8 Naar steeds persoonlijker identificatie

Als we een aantal van de genoemde kenmerken combineren (biometrie, geïntegreerde nummers, merketengebruik) zien we een langzame verschuiving optreden naar het gebruik van steeds meer op een unieke persoon toegesneden identificatiemiddelen: 'uniek' wordt steeds 'unieker'. Daarbij komt dat de diverse unieke kenmerken ook steeds vaker met elkaar in verband (kunnen) worden gebracht, waardoor weer nieuwe informatie beschikbaar komt. Illustratief zijn de koppelingsmogelijkheden van biometrie aan andere identificatie- en dossiersystemen, zoals camera's die worden gebruikt voor observatiedoeleinden.⁵ Het gevolg van deze ontwikkeling is dat overheid en bedrijfsleven steeds dichter op 'de huid' van een individuele persoon kunnen kruipen. Identiteit krijgt invulling via de verwachtingen die in een bepaalde situatie met de gebruikte identiteitsinstrumenten en de daaraan gerelateerde informatie worden opgeroepen. Maar als alle mogelijke contexten en daaraan gerelateerde informatie samensmelten, ontstaat een bijna allesomvattend beeld van iemands identiteit. Daardoor convergeert de identiteit, die in eerste instantie niet meer was dan een door de externe omgeving bepaalde afspraak, steeds meer met de unieke persoon die we zelf zijn en wensen te zijn. Waar vroeger zo'n totaalbeeld ontbrak, is het thans mogelijk de stukjes van de puzzel bijeen te brengen.

2.6 Besluit

In dit hoofdstuk hebben we gezien dat digitale identificatie in het te verwachten beleid voor de komende periode op vier leidende beleids-thema's een essentieel en strategisch element zal zijn. Ook onder de twee paarse kabinetten is hard gewerkt aan de verdere uitbouw en optimalisatie van de digitale equivalenten van onze vertrouwde – vaak op papier gebaseerde – identificatiemiddelen en er zijn de nodige Europese beleidsinitiatieven. Van een afstand biedt het beeld van de rol en toepassing van nieuwe digitale instrumenten misschien een caleidoscopische aanblik. Uit het overzicht van de belangrijkste Europese en Nederlandse beleidsinitiatieven op dit terrein blijkt echter dat wel degelijk een aantal duidelijke trends, gemeenschappelijkheden en opmerkelijkheden zichtbaar is. Waar we vervolgens voor staan is te bepalen welke fundamentele vragen en implicaties deze tendensen oproepen. Voor welke mogelijke implicaties en belangentegenstellingen komen we nu of in de toekomst te staan, en welke keuzes moeten nu – en door welke instanties – worden gemaakt?

3 Afwegingen, conclusies en aanbevelingen – een uitruil van belangen

3.1 Inleiding

Om een betrouwbaar stelsel voor digitale identificatie te ontwikkelen, zullen duidelijke keuzes moeten worden gemaakt. Maar welke precies? Welke belangen staan op het spel, waar liggen de spanningen en welke uitruil van belangen moet plaatsvinden? Naar deze vragen kijken we in dit laatste hoofdstuk. In de tweede paragraaf zullen we aan de hand van de in het vorige hoofdstuk gesignaleerde ontwikkelingen, zien dat er vier verschillende afwegingen kunnen worden onderscheiden. Aan de hand van deze afwegingen zullen we telkens de fundamentele keuzes die gemaakt moeten worden, identificeren. In paragraaf 3 beschrijven we op basis van deze keuzes welke conclusies nu te trekken zijn en welke gevolgen dit heeft voor de overheid bij de vormgeving van het beleid rond digitale identiteit.

3.2 Een viertal afwegingen

3.2.1 De infrastructuur: eenheid versus diversiteit

Het overzicht van beleidsinitiatieven in het vorige hoofdstuk laat zien dat de diverse projecten die digitale identificatie moeten verwezenlijken, tamelijk autonoom van elkaar functioneren. Er is sprake van een eilandencultuur bij het initiëren en uitvoeren van de plannen. Toch constateerden we ook dat er langzaam een tendens van ontkokering zichtbaar is. Zagen we dat voorheen de inspanningen primair gericht waren op digitale identificatiemiddelen die voor de eigen specifieke context noodzakelijk zijn, nu ligt het accent meer op de verbetering van de dienstverlening en verhoging van de efficiëntie. Daaruit vloeit de behoefte voort aan mogelijkheden om de verschillende initiatieven te coördineren en waar mogelijk op elkaar af te stemmen of te integreren. Een eenvormig systeem van digitale identificatiemiddelen heeft immers als voordeel dat meerdere gegevensbronnen op een zinvolle manier kunnen worden ontsloten.

De uiterste variant van integratie is een uniform stelsel voor digitale identificatie, waarbij de uitgifte, de keuze voor het type identificatie-

instrument en alle overige onderdelen van het stelsel rekening wordt gehouden met de afgesproken standaard. De identiteitsgegevens worden centraal beheerd, de verantwoordelijkheden met betrekking tot het stelsel liggen op een centraal niveau, de identificatiemiddelen zijn gestandaardiseerd en er zijn centrale afspraken gemaakt over een eenvormig gebruik van identificatiesleutels, zoals nummers en andere unieke kenmerken. Met een dergelijke, geïntegreerde identiteitsinfrastructuur zijn grote voordelen te behalen op het terrein van eenduidigheid, transparantie en efficiëntie.

Dat het ontwikkelen van een dergelijk stelsel zeker niet ondenkbaar is, mag blijken uit de recente initiatieven in de private sector om te komen tot een eigen systeem voor het internet. En met elke stap – hoe klein ook – in de richting van stroomlijning, coördinatie en integratie van digitale identificatie, komen we in de buurt van een uniform (nationaal) stelsel.

Maar er kleven natuurlijk ook nadelen aan een geïntegreerd systeem van digitale identificatie. Met elke verdere stap in die richting maken we ons tegelijkertijd ook afhankelijker van het adequaat functioneren van dat ene stelsel en worden we kwetsbaarder. De gevolgen van bijvoorbeeld *cybercrime*, *cyberterrorisme* en *identity theft* kunnen met een dergelijk geïntegreerd systeem veel groter zijn. De recente ontwikkelingen rondom identiteitsfraude met de pinpas, sofi-nummers en de zorgpas wijzen erop dat de ogenschijnlijk waterdichte fundamenten van onze identiteitsinfrastructuren wel degelijk scheurtjes kunnen vertonen. De situatie in de Verenigde Staten kan hier als angstaanjagend voorbeeld fungeren: daar worden jaarlijks tussen de 500.000 en 700.000 mensen het slachtoffer van identiteitsfraude en staat het bovenaan de lijst met snelstgroeiende vormen van criminaliteit (<http://www.consumer.gov/idtheft/reports/gao-d02766.pdf>).

De kwetsbaarheid neemt nog verder toe als we de controle met traditionele systemen gaan verwaarlozen. Als we de corrigerende werking van fysieke identificatie niet meer laten doorwerken, ontstaan ficties die vervolgens realiteit worden ('het staat zo in de computer, dus het klopt, mevrouwetje'). Daarom is het van groot belang na te denken over de vraag hoe lang we de fysieke reserve van onze digitale identificatiemiddelen willen (en zouden moeten) bewaren, welke (juridische) waarde we daaraan hechten, en vooral ook wat de consequenties kunnen zijn als we deze reserve verwaarlozen.

3.2.2 De zwaarte van het middel: absoluut of relatief

Een tweede afweging betreft de vraag hoe sterk het middel moet zijn. Er zijn immers verschillende sterktes. Er lijkt sprake van een 'identificatielif': steeds vaker wordt identificatie vereist en daarbij wordt het

zwaarste middel ingezet. Vraagt de overheid (en het bedrijfsleven) echter niet meer dan waar zij recht op heeft? Weegt het belang van honderd procent zekerheid op tegen de offers (privacy, kosten, moeite) die de burger zich moet getroosten? Dient het uitgangspunt te zijn dat individuen altijd identificeerbaar moeten zijn, waarbij centralisatie en stroomlijning van registraties het mogelijk maken (indien nodig en omkleed met wettelijke waarborgen) zoveel en zo snel mogelijk gegevens over een individu te verzamelen? Of moet het uitgangspunt eerder zijn dat in rechtsrelaties een gedifferentieerd en contextgebonden stelsel van bevoegdheidsvaststelling heerst, waarbij zo mogelijk een pseudoniem en niet een identiteit wordt gebruikt, en waarbij contextafhankelijke gegevens niet per se te relateren zijn aan één en dezelfde persoon (Koops 2001)?

Is de zwaarte van het middel dus een absolute, autonome grootheid of is het een variabele die, afhankelijk van de situatie waarin een vorm van 'bekendmaken' moet plaatsvinden, tot een bepaalde uitkomst leidt? Overigens moeten we daarbij ook constateren dat we ons zwaar lijken te concentreren op het middel (document of biometrie), zonder dat we ons druk maken over de vraag wat we deden – en vooral ook waaróm we dat deden – toen identificatie voor het eerst plaatsvond (de zogenaamde authenticatie, zie ook bijlage 1). We lijken daarbij te vergeten dat de sterkte van de identificatie van meer factoren afhangt dan alleen het middel dat wordt gebruikt. Juist de registratie en het beheer van identiteitsgegevens, alsmede het proces van authenticeren (dus de eerste registratie) en de organisatie van het gehele stelsel zijn cruciaal voor de betrouwbaarheid. Anders gezegd: er wordt veel waarde gehecht aan het middel en we hebben minder aandacht voor de context waarbinnen dat middel moet functioneren: zowel intern (ontwerp, beheer) als extern (de noodzaak van gebruik).

3.2.3 De regie: publiek versus privaat

De afweging die hier gemaakt moet worden, is wie het initiatief en de regie rond de vormgeving van digitale identificatie op zich moet nemen. Waar en onder welke omstandigheden moet de overheid een monopolie hebben en waar mag (of zelfs *moet*) ze ruimte laten voor marktpartijen? Voor welke sectoren? Wie zetten de standards? Waar moet de overheid handelen en waar juist niet? Hierbij komt ook de vraag naar voren wat nu precies de wisselwerking is tussen markt en overheid. De overheid zal zich bewust moeten zijn van haar verschillende rollen en haar specifieke hoedanigheid. In sommige gevallen zal immers uitsluitend de overheid in staat zijn bepaalde maatregelen te nemen, voldoende vertrouwen te geven en waarborgen te scheppen die onmisbaar zijn om digitale identificatie en identificatiemiddelen vorm te kunnen geven.

Tegelijkertijd zal de overheid scherp moeten zijn op de positie van het bedrijfsleven in samenhang met de dynamiek van de technologie: als zij dat niet doet, zal zij voor voldongen feiten komen te staan en nog maar moeilijk in staat zijn zichzelf en burgers te behoeden voor een te grote afhankelijkheid van het bedrijfsleven, die kan leiden tot een grotere kwetsbaarheid van burgers en overheid.

3.2.4 De wens: gemak en resultaat versus vrijheid

De ontwikkelingen op het gebied van de informatie- en communicatietechnologieën hebben ons maatschappelijk en sociaal functioneren de afgelopen jaren in vele opzichten eenvoudiger gemaakt. Ook de publieke sector heeft in vele opzichten zijn voordeel kunnen doen met ICT. Zo zijn de afgelopen jaren diverse ICT-applicaties ontwikkeld en ingezet om bestuurlijke problemen aan te pakken, handhaving te verbeteren en de dienstverlening efficiënter te laten verlopen. De applicaties worden daarbij veelal als service aan de burger gepresenteerd (burger-servicekaart) of geïntroduceerd onder het motto 'leuker kunnen we het niet maken, wel makkelijker'. Ook de plannen rondom identificatie en digitale identificatiemiddelen passen in dit beeld. Proactieve dienstverlening, eenmalige gegevensverstrekking, stroomlijning van gegevens: de plannen worden gelanceerd met als boodschap een verbeterde dienstverlening door de overheid.

De uiteindelijke consequentie van deze ontwikkelingen kan zijn dat de overheid de beschikking krijgt – of denkt te hebben – over een vrijwel compleet beeld van het doen en laten van haar burgers. Op eigen initiatief aanvragen van bepaalde voorzieningen hoeft dan niet meer. Bezwaar aantekenen heeft weinig zin. De overheid beschikt immers over alle relevante informatie. Binnen dit kader passen kreten als: 'Uit onze gegevens blijkt dat u recht hebt op een tegemoetkoming. Nadere informatie hebben we niet nodig. We beschikken inmiddels over alle noodzakelijke gegevens.' 'Uit onze bestanden blijkt dat deze gegevens juist zijn.' 'Indien u het met de beslissing niet eens bent, kunt u bezwaar aantekenen, maar inmiddels blijkt uit andere bronnen dat...'

De veronderstelling dat al deze informatie ook de *juiste* informatie is die conform geldende wetgeving mag worden vastgelegd, geeft de overheid de garantie dat procedures vervolgens ook efficiënt en snel kunnen worden afgehandeld. Maar het is nog maar de vraag tot hoever we optimalisatie (onder het mom van 'gemak') willen doorvoeren? Waar trekken we de grens en waar laten we het initiatief en de regie aan de burger? Kortom: wanneer krijgt vrijheid voorrang boven gemak?

3.3 Conclusies en aanbevelingen

In de vorige paragraaf hebben we gezien dat er in feite vier afwegingen zijn die gemaakt moeten worden, die lastige keuzes met zich meebrengen en waarbij tegengestelde belangen naar voren komen. Deze keuzes zijn complex en onderling sterk gerelateerd. Niettemin is een aantal aanbevelingen te geven voor het toekomstige beleid rond digitale identificatie. Daarbij zal de overheid niet alleen moeten leiden, zowel in het debat als in de uitvoering, maar tegelijkertijd ook moeten volgen.

We moeten daarbij vasthouden dat stilzitten geen optie is, want dat leidt op macroniveau tot maatschappelijk en economisch verlies. Met een goed doordacht stelsel van digitale identificatie zal de dienstverlening veel beter en efficiënter uitgevoerd kunnen worden. Voorts kan een nieuw stelsel ook sterke internationale gevolgen hebben. De aanwezigheid van zo'n stelsel kan voor bedrijven (mede) een reden zijn zich in Nederland te vestigen of het land juist te mijden. Het vormt in feite een beleidsconcurrerend instrument. Dit schept wel een verantwoordelijkheid: het zal niet mogen leiden tot ongewenste overheidsinterventies. Een ongebreidelde, ontkokerde en gekoppelde informatiegroei bij de overheid over het doen en laten van burgers is niet alleen in strijd met privacyregels, het kan gemakkelijk leiden tot een gevoel van onvrijheid. Bovendien maakt clustering ook kwetsbaar in de zin dat de zwakste schakel de betrouwbaarheid en veiligheid van de gehele keten bepaalt. We zullen daarom moeten bewegen, niet overhaast, slordig of gefragmenteerd, maar wel doordacht.

3.3.1 De overheid moet volgen

Er zal een overkoepelend goed doordacht stelsel voor digitale identificatie moeten komen (regels, infrastructuur, processen). De overheid zal echter, gezien de complexiteit van de materie en zeker in het tijdsgewricht waarin wij ons thans bevinden, moeten waken voor ondoordacht, overhaast en sectoraal handelen. De spanningsvelden die we geschetst hebben, geven aan dat er een groot aantal tegenstrijdige belangen speelt. Maar lang niet alle belangen lijken thans goed behartigd te worden in het politieke debat: er ontbreekt een aantal spelers op het veld, die ook bij het spel betrokken moeten worden, zoals wetenschappers en hoeders van de belangen van burgers (klantvriendelijkheid) en bedrijfsleven.

Daarbij speelt tevens een rol dat de (wetgevings)dossiers verdeeld zijn over verschillende departementen. Het ministerie van Justitie is bevoegd op het gebied van regelgeving over opsporing en privacy, Economische Zaken heeft belangrijke interesses in (de economische implicaties van het gebruik van) chipkaarten en infrastructuren en

Binnenlandse Zaken heeft, behalve de algemene coördinatie van de elektronische overheid, ook de introductie van regels rond (bron-)identiteitsmiddelen in zijn portefeuille. Daar komt nog bij dat de (bredere) beleidsacties over een nog groter aantal departementen zijn verdeeld.

Deze materie vereist daarom een geïntegreerde, departementoverschrijdende aanpak. Op dit moment ontbreekt het echter nog aan de structuren en aan de broodnodige inzichten. Beleidsinterventies zijn daarom in het beste geval eenzijdig, niet-effectief en disproportioneel. In het slechtste geval kunnen zij zelfs contraproductief blijken en ons opzadelen met hindernissen die het scheppen van een noodzakelijk stelsel (met alle waarborgen daaromheen) alleen maar bemoeilijken.

3.3.2 De overheid moet het debat leiden

Maar de overheid moet niet alleen een meer afwachtende houding aannemen. Ze zal tegelijkertijd moeten handelen. De initiatie en de verdere vormgeving van het integrerende debat is bij uitstek iets wat bij de overheid ligt: een andere partij zal dit, denkend vanuit een deelbelang, niet kunnen. Uiteindelijk moet het integrerende debat tot een langetermijnvisie leiden. Maar hoe moet een dergelijk debat eruitzien? Vier punten zijn daarvoor van belang.

Langetermijnontwikkelingen moeten leidend zijn

Allereerst moet vastgesteld worden dat de beoogde beleidsdoelstellingen voor digitale identificatie (nu in Nederland onder andere veiligheid en vreemdelingenbeleid) wellicht aan verandering onderhevig zijn, maar dat de ontwikkelingen die we in hoofdstuk 2 hebben gezien dezelfde blijven, zoals bijvoorbeeld het gebruik van biometrie, toenemende ontkokering, centralisatie en koppeling van gegevens. Dat betekent in ieder geval dat ook bij de vormgeving van het kortetermijnbeleid, de langetermijnontwikkelingen de koers dienen te bepalen, en niet omgekeerd. Daar komt nog bij dat het gehele proces een eigen dynamiek kent: een aantal van de – onder de paarse kabinetten – in gang gezette ontwikkelingen is onomkeerbaar. De oorspronkelijke beleidsdoelstellingen die er aan ten grondslag lagen zijn inmiddels misschien wat naar de achtergrond verdwenen, maar het veranderingsproces gaat gewoon door. Deze ontwikkelingen zullen het debat structureel blijven sturen.

Het debat moet zich losmaken van de focus op middelen

We hebben er eerder op gewezen dat er sprake is van een spraakverwarring, dat de begrippen identiteit, identificatie en middel door elkaar worden gebruikt. Uit de verschillende initiatieven blijkt echter dat het debat en de beleidsacties zich uitsluitend concentreren op het middel en het proces. Over de implicaties van (het scheppen van) die middelen, wordt daarentegen te weinig nagedacht. Dit heeft tot gevolg dat

de achterliggende en veel fundamentele discussie over de consequenties van de inzet van deze middelen voor het identificatieproces, en uiteindelijk voor hetgeen we verstaan onder onze identiteit, niet of onvoldoende wordt gevoerd. Ook is er nog te weinig nagedacht over het scheppen en vooral het beheer van het stelsel. Wie moet dat doen? Welke waarborgen moeten gelden? Hoe moeten onderhoud en beveiliging vorm krijgen en welke regels en *checks and balances* moeten er gemaakt worden om het ontstaan en voortbestaan van juridische ficties tegen te gaan? Moet de belangenafweging meer in het voordeel van privacy uitvallen, of moeten we de lat voor privacybescherming nu juist wat lager leggen? De overheid moet er kortom voor zorgen dat er een discussie ontstaat over de fundamentele veranderingen die optreden bij de nieuwe invulling van identificatie en identificatieprocessen. Ze moet zich niet uitsluitend druk maken over de vraag of er nu wel of geen biometrische kenmerken op de chipcard moeten zitten.

Het debat moet open zijn

We hebben gezien dat er binnen de gestelde kaders sprake is van grote belangentegenstellingen. Heeft eenheid of juist diversiteit de voorkeur? Moet de publieke sector de regie voeren of is er ook een rol voor de private sector? Moet gekeken worden naar efficiency of juist naar gebruikersgemak? Is er altijd honderd procent zekerheid nodig over iemands identiteit of kunnen we in bepaalde gevallen ook met minder zekerheid genoegen nemen? Om een voldoende doordacht antwoord op deze en andere vragen te kunnen geven, moet het debat open zijn. Proportionaliteit en subsidiariteit moeten steeds in acht genomen worden: is het beleidsinstrument niet te zwaar? Is er geen andere weg mogelijk, die minder ingrijpend is? Dit geldt des te meer als wij ons realiseren dat het *scheppen* van bepaalde identificatiemogelijkheden leidt tot het *gebruik* ervan, ook in contexten waarvoor ze oorspronkelijk niet bedoeld waren. De exacte toekomstige applicaties en implicaties zijn daardoor moeilijk te voorspellen. Dit hebben we gezien bij de ontwikkeling van het sofi-nummer: wie had destijds kunnen verwachten dat dit de functie zou krijgen die het momenteel heeft, en dat het aan de basis zou komen te staan van het nieuwe Burger Service Nummer?

Het debat moet leiden tot een gedragen visie die aanzet tot handelen

Het voeren van het voornoemde debat is uiteraard geen doel op zich: uiteindelijk moet het leiden tot een visie die de eroderende werking van de politieke kortetermijnplannen en de waan van de dag kan doorstaan. In deze visie moeten de diverse belangen op een gebalanceerde wijze zijn uitgewisseld en verdisconteerd. Vervolgens zal ook gehandeld moeten worden: de visie moet vertaald worden naar een solide stelsel van digitale identificatie. Hoe meer draagvlak er is voor de visie, des te eenvoudiger zal de implementatie ervan zijn.

3.3.3 De overheid moet handelen

De overheid kan echter niet volstaan met uitsluitend initiëren en leiden van het debat. Op sommige vlakken zal zij ook handelend moeten optreden. Zij zal daarbij moeten balanceren, coördineren en, niet in de laatste plaats, beschermen en onderzoeken.

Onderzoek naar burgerbeleving

De overheid is er voor de burger. Daarom is het raadzaam meer onderzoek te doen naar de burgerbeleving van digitale identificatie. Gedacht vanuit het *contrat social* zouden de uitkomsten hiervan een belangrijk ijkpunt moeten zijn om beleid vorm te geven. Helaas is voor dergelijk onderzoek in ons land nog weinig aandacht en ruimte, in tegenstelling tot bijvoorbeeld de Angelsaksische landen. Wel is onderzoek gedaan naar de privacybeleving van burgers, in het verleden door het Rathenau Instituut en recentelijk nog door Koops en Vedder.⁶ Naar aanleiding van actuele problemen laten dagbladen ook dikwijls enquêtes uitvoeren naar de meningen van burgers over bijvoorbeeld de geloofwaardigheid van bepaalde opsporingsactiviteiten. Structureel onderzoek naar de opvattingen van burgers over digitale identificatie ontbreekt echter tot op heden.

Checks and balances introduceren

De overheid kan steeds meer te weten komen over de personen met wie ze te maken krijgt. Ze gaat als het ware steeds dichterbij de burger zitten. Er ontstaat bovendien een stelsel waarin identificatie ook steeds betrouwbaarder, verfijnder en detaillistischer kan worden. Stonden de verschillende systemen vroeger los van elkaar en waren ze feilbaar, nu zijn ze steeds beter te koppelen en functioneren ze praktisch feilloos. Bovendien zien we dat de overheid, vanuit de gedachte van stroomlijning en eenmalige gegevensverstrekking, de verzamelde informatie voor andere taken gaat gebruiken dan de taak waarvoor ze die in eerste instantie heeft verkregen. Binnen die contouren dient de overheid wel een systeem van checks and balances te introduceren. Koppelen vergroot de afhankelijkheid van de betrokken personen. De overheid moet daarom een hoog kwaliteitsniveau waarborgen: een soort digitaal voorzichtigheidsbeginsel, gekoppeld aan een hoge mate van juridische precisie.

Een structuur voor coördinatie

We hebben gezien dat er inmiddels enkele voorzichtige pogingen worden gedaan om te komen tot een betere coördinatie van beleid en initiatieven. Uiteraard is dit toe te juichen, maar het is zeer de vraag of dit voldoende zal zijn. De belangentegenstellingen zijn immers groot en er zit een scala aan deelnemers aan de beleidstafel. Als er coördinatie is, lijkt dit vaak sector- en themabepaald. De coördinatie dient veel meer plaats te vinden op een hoger en algemener beleidsniveau. Er bestaat echter geen structuur, laat staan een bestuurlijke entiteit,

die een geïntegreerde analyse of evaluatie mogelijk maakt. Een dergelijke structuur zou de broodnodige diversiteit aan invalshoeken kunnen verschaffen. Zo zouden er binnen een dergelijk kader ook afspraken gemaakt kunnen worden over meldingsplichten rond beleidsinitiatieven en rapportages. Wellicht zou een dergelijke taak ondergebracht kunnen worden bij een bestaande instantie, bijvoorbeeld het College Bescherming Persoonsgegevens, maar het valt zeker te overwegen een organisatie als het ICTU hiermee te belasten.

Publiek-private samenwerking

Zoals in de inleiding is aangegeven, is het scheppen en het beheer van het stelsel van digitale identificatie een collectief goed. De overheid zal in dat kader haar monopolie niet zonder meer prijsgeven. Toch is geenszins denkbeeldig dat dit (gedeeltelijk) gebeurt. De markt zit niet stil en er worden standaards ontwikkeld die ook bepalend zijn voor de overheidsdienstverlening, zoals de parkeermeters in Rotterdam, de discopas, de zorgpas, de digitale kluisjes van de ANWB en de irisscan op Schiphol. Dit heeft ook consequenties op technologisch niveau: als de leidende applicaties allemaal met een irisscan werken, wat wil de overheid dan nog beginnen met een vingerafdruk?

Het is dus van groot belang dat de overheid steeds doorgrondt wat de mogelijke toekomstige implicaties van private identificatie-initiatieven kunnen zijn voor de eigen vormgevingsactiviteiten. Men moet overigens niet vergeten dat de *toekenning* van digitale identificatiemiddelen (en het beheer van het identificatiesysteem) een andere zaak is dan het daadwerkelijke *gebruik* van die middelen. Door de overheid gecreëerde digitale identificatiemiddelen kunnen wel degelijk in de private sector een rol spelen. Het scheppen en toekennen van de bronidentiteit (met behulp van bijvoorbeeld biometrie) moet echter voorbehouden blijven aan de overheid, terwijl de private sector wel gebruik kan maken van de *templates*, maar niet van de achterliggende gegevens. Er zijn interessante publiek-private samenwerkingsvormen denkbaar en misschien zijn deze zelfs wel noodzakelijk.

3.4 Epiloog

Een betrouwbaar stelsel voor digitale identificatie vereist doordachte en duidelijke keuzes van de overheid. Kiezen veronderstelt een bewustzijn van de aanwezigheid van verschillende opties en een analyse van de belangen die op het spel staan. We hebben in dit hoofdstuk gezien dat een dergelijke belangenafweging nog onvoldoende wordt gemaakt: een totaaloverzicht ontbreekt, de initiatieven zijn veelal sectoraal ingekleurd en sommige belangenvertegenwoordigers zitten nog niet eens aan de onderhandelingstafel. Dit wordt hoog tijd.

We zien immers dat op tal van fronten *points of no return* bereikt worden. Zo is het nummerbeleid in een spectaculaire stroomversneling geraakt en zullen er op korte termijn belangrijke beslissingen genomen moeten worden op het gebied van onze identiteitskaart (biometrische toepassingen incorporeren of niet?). Tevens mag verwacht worden dat het voornemen een algehele identificatieplicht in te voeren (en vooral de sancties als hij niet wordt nageleefd), tot enkele stevige debatten zal leiden. In dat kader zien we dat de echo's van 11 september 2001 langzaam wegsterven en wordt de kritiek op de indringender handelende – en opsporende – overheid steeds luider. Verder op de achtergrond sluipt de kwestie van de regie: blijft de overheid de baas of wordt zij straks binnendoor ingehaald door (de facto) standaards van het bedrijfsleven?

Van een hoedende en waakzame overheid – en anders wel van een oplettend parlement – mogen we verwachten dat zij de discussies die in tal van arena's gevoerd worden of gaan worden, met elkaar in verband brengt. Zeker als we bedenken dat het hier gaat om een van de meest fundamentele inrichtingselementen van onze samenleving: onze (digitale) identiteit en alles wat daaromheen cirkelt. Op naar een betrouwbaar stelsel: een stelsel van digitale identiteit!

Bijlage 1

Identiteit, identificatie en middel

Inleidende opmerkingen

Deze bijlage dient om een duidelijker beeld te scheppen van de kernbegrippen die in deze studie zijn gehanteerd. Kijkend naar de diverse beleidsstukken, de publicaties in de pers en wetenschappelijke literatuur, valt namelijk direct op dat wanneer wordt gesproken over het begrip 'digitale identiteit' een scala aan termen opduikt. Bovendien bestaat er allesbehalve eenduidigheid over de exacte betekenis van deze termen.

Een belangrijke oorzaak van de spraakverwarring ligt in het feit dat vaak geen onderscheid wordt gemaakt tussen het *concept* identiteit, het *proces* van identificatie en het *middel* dat daarbij wordt gebruikt. Het is voor de politieke, wetenschappelijke en maatschappelijke discussie over (de toekomst van) digitale identificatie wel noodzakelijk om het verschil tussen deze drie dimensies duidelijk te onderkennen.⁷

Identiteit

Identiteit wordt sterk door de specifieke context bepaald en ingekleurd. Identiteit kan daarom wellicht het best worden omschreven als verwachtingen die in een bepaalde situatie met de gebruikte identiteitsinstrumenten en de daaraan gerelateerde informatie worden opgeroepen.

Wanneer we het hebben over het kenbaar maken van onze identiteit, denken we meestal aan het noemen van onze naam. Van oudsher is onze naam inderdaad een belangrijk instrument om te kunnen functioneren in de maatschappij. Identificatie werd, en wordt nog steeds, meestal verricht op basis van een naam of visuele herkenning. Iemand aanwijzen en zeggen 'dat is Jan Niemandsland' wijst er voor velen op dat de identiteit van een persoon is vastgesteld en we te maken hebben met een *geïdentificeerd persoon*. We kunnen immers een naam plakken op de persoon in kwestie. Kortom, onze naam blijkt – vaak in combinatie met diverse andere kenmerken – in ons dagelijks leven een belangrijk identificatiemiddel.

Toch is onze naam zeker niet gelijk aan onze identiteit. Denkend over een goede omschrijving van identiteit, constateren we dat het bijna

een even diffuus en moeilijk te omschrijven begrip is als privacy. Net als privacy lijkt ook de invulling van het begrip identiteit sterk door de specifieke context te worden bepaald en ingekleurd. Identiteit kan daarom wellicht worden omschreven als de verwachtingen die in een bepaalde situatie met de gebruikte identiteitsinstrumenten en de daaraan gerelateerde informatie worden opgeroepen. Daarbij kunnen we beschikken over een juridische identiteit, een administratieve identiteit of bijvoorbeeld een medische identiteit. Identiteit staat daarmee ook buiten ons als persoon: het is slechts een door de buitenwereld gegenereerde afbeelding van ons. Identiteit is soms dan ook niet meer dan een afspraak.

Maar behalve de sterk contextuele – en daarmee door de buitenwereld bepaalde – inkleuring van het begrip identiteit, kennen we het begrip ook in de zin van de unieke persoon die we zelf zijn en wensen te zijn (onze ‘ik’). We hebben het dan over het beeld dat we van onszelf en over onszelf hebben. In feite betekent dit dat het begrip identiteit twee gedaantes kent: een uiterlijke, voor een belangrijk deel door de externe omgeving bepaalde en opgelegde identiteit, en een innerlijke, in essentie primair door onszelf bepaalde identiteit. Deels interfereren deze beide identiteiten natuurlijk (kleren maken nu eenmaal de man).

Zoals gezegd wordt onze identiteit vaak ontleend aan een bepaalde bron. Dat kunnen publieke bronnen zijn, maar ook particuliere bronnen. Vanaf het moment van aangifte bij een gemeente na de geboorte, is de bevolkingsadministratie de meest centrale en doorslaggevende bron van onze identiteit. Vele andere bronnen zijn een afgeleide van de bevolkingsadministratie of ontlenuen hun informatie om te fungeren als identiteitsbron aan deze administratie. Ook voor de toekenning van ‘digitale identiteiten’ is de publieke sector de meest vooraanstaande bron. De particuliere pendanten van identiteitsbronnen zijn veelal beperkt in functie, tijd en reikwijdte van gebruik.

Ten slotte moet hier worden vermeld dat we behalve het begrip identiteit, ook termen als pseudo-identiteit en pseudoniem tegenkomen. Reeds decennialang wenst de mens zijn of haar naam en daarmee identiteit in bepaalde situaties verborgen te houden. Soms wil men daarbij volledige verhulling nastreven, soms wil men zich echter toch (her)kenbaar maken. De bekendste voorbeelden van deze laatste categorie zijn te vinden in de literaire en muziekwereld. Schrijvers en muzikanten wensen weliswaar hun ware naam niet te onthullen, maar willen zich wel naar een grotere groep individualiseren (en aldus met hun werk herkenbaar zijn). Daarom hanteren ze een pseudoniem als middel voor herkenning. Ook in een elektronische omgeving wensen mensen soms anoniem, maar toch herkenbaar te zijn. Een voorbeeld is ‘chatten’. In dit geval gaat het ook om de algemene bekendheid onder het pseudoniem (veelal ‘nym’ genoemd). We staan hier verder niet stil bij ontwikkelingen rondom pseudo-identiteit en pseudoniem.

Identificatie

Identificatie is het proces waarbij aan de hand van identiteitskenmerken in combinatie met identificatiemiddelen een bepaald persoon kenbaar en herkenbaar wordt gemaakt.

Met andere woorden, bij identificatie relateert men bepaalde informatie aan een bepaalde identiteit en wordt vastgesteld of de door een persoon gebruikte identiteit ook werkelijk bij hem of haar hoort. Daarmee is echter nog niet gezegd dat ook is vastgesteld of het om die ene unieke persoon gaat. Kortom, waar in het algemeen spraakgebruik bij de term identificatie meestal wordt aangenomen dat een persoon uniek kenbaar en herkenbaar voor de ander wordt, ligt de werkelijkheid toch vaak veel genuanceerder. Al eerder werd door het College Bescherming Persoonsgegevens een onderscheid gemaakt tussen *identificatie*, het vaststellen van iemands identiteit, en *authenticatie*, het vaststellen dat iemand is wie hij of zij claimt te zijn.⁸

In diverse documenten wordt vaak gesproken over de tegenstelling tussen identificatie en anoniem kunnen handelen. Identificatie en het opheffen van anonimiteit zijn echter zeker niet elkaars tegenpolen. Ook de achterliggende behoeften bij de inzet van identificatie is niet een kwestie van twee uitersten. In sommige gevallen is geen behoefte aan het doorbreken van anonimiteit, in andere gevallen volstaat het dat er een aanknopingspunt bestaat om zo nodig een persoon aan te spreken, in weer andere gevallen is er niet alleen behoefte aan identificatie van (sporen van) een persoon, maar ook aan verificatie van de ware identiteit van één bepaald persoon. Voor dit laatste is meer nodig dan een controle van identiteitskenmerken. Er moet sprake zijn van een combinatie met zwaardere identiteitskenmerken, dat wil zeggen met kenmerken die meer vertegenwoordigen dan een 'afpraak'.

Het verschil tussen de gradaties van identificatie schuilt dus in de gezochte graad van zekerheid over de ware identiteit van de wederpartij, waarbij identificatie in combinatie met authenticatie pretendeert de meeste zekerheid te geven over de vraag of iemand is wie hij of zij claimt te zijn. Authenticatie vormt dus als het ware een soort *double check* op de identificatie. De huidige maatschappelijke behoefte om deze extra zekerheid te krijgen, verklaart de roep om het gebruik van biometrie en DNA als identificatiemiddelen.

Identificatiemiddel

Onze naam en ons uiterlijk vormen van oudsher belangrijke middelen voor het vaststellen van onze identiteit. Inmiddels lijken deze middelen echter te worden verdrongen door digitale pendanten,

zoals biometrie, DNA, wachtwoorden, pin, chipkaarten, passen en andere dragers van identiteitskenmerken en immateriële codes.

In onze huidige informatiemaatschappij zijn we voor ons dagelijks doen en laten bijna volkomen afhankelijk geworden van een scala aan digitale en veelal dwingend opgelegde instrumenten om aan te tonen wie we zijn. Onze naam is daarbij allang niet meer het meest geschikte, gewenste en vereiste instrument om ons te identificeren. Maar ook degene die een dagelijks gebruiksmiddel als een bankpas is kwijtgeraakt, zal constateren dat geld opnemen met behulp van een vervangend identificatiemiddel dat onze naam en uiterlijk toont (paspoort) zeker niet vanzelfsprekend is. De onrust die ontstond naar aanleiding van de fraude met pinpassen in de zomer van 2002, laat ook zien hoe kwetsbaar ons vertrouwen in deze identificatiemiddelen is.

Illustratief voor de nieuwe situatie is de definitie van persoonsgegevens in de Wet bescherming persoonsgegevens (Wbp): "Iedere informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon, hierna 'betrokkene' te noemen; als identificeerbaar wordt beschouwd een persoon die direct of indirect kan worden geïdentificeerd, vooral aan de hand van een identificatienummer of van een of meer specifieke elementen die kenmerkend zijn voor zijn of haar fysieke, fysiologische, psychische, economische, culturele of sociale identiteit." Uit deze definitie volgt dat er inmiddels vele andere identificatiemiddelen zijn dan de naam. Het identificatienummer krijgt zelfs een wat aparte vermelding. Dat is niet toevallig, gezien het gretige gebruik dat onze samenleving maakt van nummers om mensen te identificeren. Familie- en voornamen zorgen immers voor verwarring, terwijl nummers uniek kunnen zijn.

Behalve nummers zijn diverse andere (digitale) identificatiemiddelen in gebruik of in opkomst. Deze middelen zijn in talrijke groepen onder te verdelen. Zo zijn er persoonsgebonden (biometrie, DNA) en niet-persoonsgebonden methoden (wachtwoord, pin), materiële (chipkaart, pas en andere dragers van identiteitskenmerken) en immateriële methoden (code), kenbare en niet-kenbare methoden, wilsafhankelijke (intypen van een code) en wilsonafhankelijke methoden (camera), actieve en passieve methoden. Van alle nieuwe identificatiemiddelen staan momenteel vooral biometrie en DNA in de belangstelling. Biometrie maakt gebruik van lichaamskenmerken van een individu, zoals de vingerafdruk en iris. Deze kenmerken zijn uniek toe te schrijven aan de drager en juist het unieke van deze kenmerken maakt ze geschikt om absolute zekerheid te verkrijgen met wie precies men van doen heeft.

Bijlage 2

Overzicht geïnterviewde personen en deelnemers workshop

Geïnterviewde personen

In totaal zijn tussen november 2001 en februari 2002 tien interviews afgenomen met experts op relevante beleidsgebieden. Het gaat om de navolgende personen:

Dhr. M. Wessling	Bits of Freedom
Mr. J.E. Geuzinge	GBA Amsterdam
Prof.mr. J.M.A. Berkvens	Rabobank
Mr. U. van de Pol en	
Dr. J.A.G. Versmissen	College Bescherming Persoons- gegevens
Ir. R.J. van Munster	TNO-TPD
Dr. P.H.H. Zeef	Ministerie van Sociale Zaken en Werkgelegenheid
Mw. I.H. Stempels-Dijkstra	ICTU, Taskforce PKIoverheid
Mw. mr. J.M. Titulaer-Meddens	Ministerie van Volksgezondheid, Welzijn en Sport
Dr. J.H.A.M. Grijpink	Ministerie van Justitie

Deelnemers workshop 13 mei 2002

Workshopleider

Prof.dr. A. Zuurmond Zenc BV

Experts

Mw. drs. E.W. Gommans-de Bruin	Interpay Nederland BV
Mr. J.E. Geuzinge	GBA Amsterdam
Drs. S.B. Luijtjens	ICTU – Programmabureau Stroomlijning Basisgegevens
Drs. D. Schravendeel	ICTU – Programmabureau Stroom- lijning Basisgegevens
Dr. J. Holvast	Holvast & Partner
Mr. M. Gerrard	ICTU – Taskforce PKIoverheid

Studieteam

Mw. drs. M. Schoenmacker	Rathenau Instituut
Drs. D.W. van Harten	Rathenau Instituut
Mw. prof.mr. J.E.J. Prins	Universiteit van Tilburg
Mw. M.M. Prinsen	Universiteit van Tilburg
Mr. M. de Vries BA	Universiteit van Tilburg

Bijlage 3

Overzicht van beleidsinitiatieven naar initiatiefnemers

Onderstaande tabel geeft een overzicht van de initiatieven rond digitale identiteit, gegroepeerd naar initiatiefnemer.

Naam van het initiatief en initiatiefnemer	Kern van het initiatief	Vindplaats
Europese Unie: Richtlijn elektronische handel	Ter implementatie stelt het wetsontwerp uit januari 2002 onder meer dat bij het aangaan van de elektronische overeenkomst de <i>identiteit</i> van partijen met voldoende zekerheid vast te stellen moet zijn.	richtlijn 2000/31/EG, PbEG L 178 en (2)
Europese Unie: Richtlijn elektronische handtekening	De richtlijn bevat gedetailleerde regels over de juridische erkenning en de betrouwbaarheid van elektronische handtekeningen. Op 18 mei 2001 is een wetsvoorstel ingediend ter implementatie van deze richtlijn.	richtlijn 1999/93/EG, PbEG L 13
Europese Unie: Schengen Informatie Systeem	Het Schengen Informatie Systeem is een Europese databank. Het registreert <i>real time</i> in alle aangesloten landen gegevens over gezochte personen en vermiste voorwerpen. Het wordt gebruikt door autoriteiten die zijn belast met grenscontroles.	Schengen-akkoord van 14 juni 1985 en het uitvoeringsakkoord van Schengen van 19 juni 1990
Europese Unie: Europese gezondheids- kaart	Ter vervanging van het bestaande papieren gezondheidsformulier (E-111) kan met deze elektronische kaart de burger in heel de EU het recht op gezondheidszorg aantonen. Op deze kaart zullen geen medische gegevens worden opgeslagen.	www.emanet.org/Pages/Dutch/ShortAbout.htm
Europese Unie: Europese raadpleging digitale identiteit	Begin 2002 werd onder het Spaans voorzitterschap van de Unie onder de lidstaten een enquête gehouden over hun behoefte aan coördinatie door de EC van verschillende nationale ontwikkelingen in de richting van digitale identificatiesystemen.	Cordis focus – nummer 191, p. 3 en www.cordis.lu/spain
BZK/ICTU	Advies van de Tafel 'Persoonsnummerbeleid in het kader van identiteitsmanagement', gericht op het tot stand brengen van het Burger Service Nummer (BSN).	www.stroomlijningbasisgegevens.nl/projecten/bel.shtml

Naam van het initiatief en initiatiefnemer	Kern van het initiatief	Vindplaats
BZK: Digitaal kluisje	De Commissie-Snellen heeft voorgesteld iedere burger een digitale kluis te geven waarin individuele persoonsgegevens (GBA, medische en financiële gegevens) beveiligd en versleuteld opgeslagen kunnen worden. Het geeft burgers inzicht in de persoonsgegevens die de overheid gebruikt en de mogelijkheid deze aan derden te verstrekken. Dit kluisje zou in de vorm van een chipcard met biometrische gegevens uitgegeven worden.	www.gba.nl/documentatie.htm
BZK: Haalbaarheidsstudie biometrie in reisdocumenten	Voorjaar 2003 zal BZK met de resultaten van een haalbaarheidsstudie komen naar het gebruik van biometrie in reisdocumenten. De verwachting is dat daar concrete aanbevelingen in zullen zitten voor nadere actie.	www.bprbzk.nl/downloads/020703.Brief%20TK%20biometrie.pdf
BZK: de nieuwe generatie reisdocumenten	Sinds 1 oktober 2001 geeft BZK een nieuwe reeks Nederlandse reisdocumenten uit. Naast de nieuwe vormgeving worden de reisdocumenten op één centraal punt voorzien van variabele gegevens. Ze zijn technisch beter beveiligd en bieden de mogelijkheid om in een later stadium een chip te kunnen aanbrengen voor de toepassing van onder meer biometrie. De paspoort-uitvoeringsregelingen zijn in dit kader herzien.	www.bprbzk.nl/
BZK: Negatief basisregister paspoorten en aanpassing paspoortwet	Dit pakket maatregelen verschaft de instanties belast met de uitvoering van de Paspoortwet een beter instrumentarium (juridisch en praktisch) om effectiever te kunnen optreden tegen fraude.	Wijziging van de paspoortwet Stb. 132, 2001
BZK: PKI overheid	Oprichten van een hiërarchische of horizontale (infra)structuur van certificatieaanbieders (CA's), waarbinnen architectuur, organisatie, PKI met elektronische handtekening, elektronische identiteit en vertrouwelijke elektronische communicatie een plaats moeten krijgen. Eind 2002 moet een pakket van eisen en een blauwdruk gereed zijn, die het kader zullen vormen voor een PKI die 90% van alle communicatie van burgers en bedrijven met de overheid kan faciliteren.	www.pkioverheid.nl
BZK: Stroomlijning basisgegevens	Ter verbetering van het functioneren en de informatiepositie van de overheid wordt met dit programma het stroomlijnen van basisregistraties geïnitieerd en gestimuleerd. Hiertoe worden diverse authenticatie registraties opgezet. Het programma is eind 2002 afgerond.	www.stroomlijningbasisgegevens.nl

<i>Naam van het initiatief en initiatiefnemer</i>	<i>Kern van het initiatief</i>	<i>Vindplaats</i>
BZK: Overheidsloket 2000	Beoogd wordt de publieke dienstverleners te ondersteunen bij de migratie naar een vraag-gerichte en geïntegreerde dienstverlening. Het gaat uit van de één-loketgedachte. Eind 2002 loopt dit programma af.	www.ol2000.nl
BZK: Modernisering GBA	Doel is dat het GBA zich de komende jaren gaat ontwikkelen tot een volwaardig instrument voor identiteitsmanagement. In dat kader zal de Landelijke Raadpleegbare Directory worden gerealiseerd (planning 2004), als voorloper van online beschikbaarheid van GBA (planning 2009).	www.bprbzk.nl
BZK: Registratie van probleem- jongeren	Doel van het initiatief is te komen tot een gezamenlijk registratiesysteem, zodat de verschillende instellingen gegevens kunnen uitwisselen.	
SZW: Cliënt-vol- communicatie- stelsel (CVCS)	Dit project beoogt samenwerking en communicatie te faciliteren tussen de verschillende instanties binnen de sociale zekerheid. Er loopt momenteel een pilot in het Centrum voor Werk en Inkomen in Nijmegen.	www.internetenopenbaarbestuur.nl/objects/07_koppe.pdf
SZW en Financiën: Taskforce sofi-fraude	Naar aanleiding van de UWV-rapportage over sofi-fraude is een taskforce opgericht om op korte termijn maatregelen te nemen ter voorkoming en opsporing van deze fraudes	
ZW: RINIS	Deze stichting faciliteert sectorale gegevens-uitwisseling in het sofi-domein. Doel is fraudebestrijding en verhoging van de doelmatigheid. De RINIS-servers zorgen voor een veilige uitwisseling van berichten.	www.rinis.nl
Volksgeneeskunde: Elektronisch patiëntendossier (EPD)	Dit initiatief is erop gericht binnen drie jaar een landelijke structuur te hebben waarmee bevoegde zorgverleners en apothekers inzicht kunnen krijgen in het medicatiegebruik van hun patiënt onafhankelijk van de setting en locatie waarin dit is voorgeschreven.	www.minvws.nl/document.html?folder=393&page=13805
Volksgeneeskunde: Parkinson-pas	Met deze chipcard met biometrische technologie kunnen patiënten zich bij zorgverleners identificeren. Deze dient tevens als dossier voor medische gegevens en medicijngebruik. Er draait een proef bij drie apotheken in Alphen a/d Rijn.	www.npcfcursus.nl/congres/ICTNaastJeBed.htm
VenW: Chauffeurspas voor taxichauffeurs	Deze pas dient als identificatiebewijs om zo de herkenbaarheid van chauffeurs te vergroten. Op de pas staan een foto, nummer, naam en geboortedatum.	www.taxiwet.nl/download/wetpersvervoersamenv.pdf

Naam van het initiatief en initiatiefnemer	Kern van het initiatief	Vindplaats
VenW: Elektronisch autokenteken	Beoogd wordt auto's een elektronische identiteit te geven door een op afstand afleesbare chip in elk voertuig te monteren.	www.rdw.nl/jaarverslag2001/jv2001-331.htm
Justitie: Wettelijke identificatieplicht	Sinds begin 2002 bestaat er bij dreiging van terrorisme een identificatieplicht. Er bestaan thans plannen te komen tot een algehele identificatieplicht.	www.justitie.nl/nieuws/080302pmbeperkteuitbreidingidentificatieplicht.asp
Justitie: Wet DNA	Sinds eind 2001 bestaat er voor misdrijven waarop een gevangenisstraf van vier jaar of meer staat, de mogelijkheid DNA-materiaal af te nemen	Wijziging regeling DNA-onderzoek in strafzaken, Stb 335, 2001
Justitie (1)Vreemdelingenkaart en (2) Asielpas	De vreemdelingenkaart dient ter identificatie van alle in Nederland legaal verblijvende vreemdelingen en (2) de asielpas regelt de toegang tot de asielzoekerscentra. (1) is een kaart met een foto, zonder biometrie en (2) bevat een vingerafdruk als biometrisch kenmerk op de kaart.	
Justitie: Previumpas Schiphol	Deze chipcard faciliteert snel instappen op Schiphol. Door irisherkenning vindt identificatie plaats. De proef liep tot oktober 2002.	nieuws.surfnet.nl/nieuws/hws/jg01-02/11.html
Justitie: Verwijsindex personen (VIP)	Met dit systeem wil justitie de uitwisseling van gegevens tussen de organisaties in de strafrechtelijke keten ondersteunen.	
OcnW: Onderwijsnummer	Op grond van de Wet onderwijsnummer (eind 2001) is een persoonsnummer voor het onderwijs ingevoerd, waardoor de efficiëntie kan worden vergroot. Dit nummer is gekoppeld aan het sofi-nummer.	Stb. 681, 2001
OcnW: Multifunctionele studentenchipkaart	Studenten kunnen zich met deze chipcard identificeren, betalingen verrichten en toegang krijgen tot de gegevens van de Informatie Beheer Groep.	
EZ: Overheidsformulieren online	Dit initiatief beoogt de administratieve lasten van het bedrijfsleven terug te dringen door het gebruik van standaardformulieren met behulp van internet.	www.minez.nl/ondernemers/online.htm
Defensie:	Besloten is om het militair paspoort te vervangen door een multifunctionele chipkaart. De Koninklijke Landmacht is inmiddels begonnen met de uitvoering van een project.	
VenW: OV-kaart	Dit initiatief beoogt een smartcard met een chip op de OV-kaart aan te brengen waarmee elektronisch, met behulp van een paslezer, kan worden betaald in de trein.	

Noten

1. Andere indelingen zijn uiteraard ook denkbaar: in het NCP-chipkaartonderzoek bijvoorbeeld worden de smartcardinitiatieven van de overheid besproken al naargelang de functies die ermee worden nagestreefd.
2. Het A-nummer wordt door een gemeente toegekend aan een natuurlijk persoon bij geboorte of vestiging in Nederland op grond van een geboorteakte, of aangifte van een betrokkene (of diens vertegenwoordiger), of ambtshalve. Het sofi-nummer was van oorsprong een intern nummer van de belastingdienst, dat sinds 1988 ook buiten de fiscale sfeer wordt gebruikt (sociale zekerheidssector). Vanaf 1996 is dit nummer ook opgenomen in het paspoort en het rijbewijs. Hierdoor kan het nummer door allerlei instanties overgenomen worden (mits rechtmatig). Zie verder Van Arkel et al. (1990), p. 4 met verwijzing naar Gooren & Schalk (1988). *Registraties geregistreerd* en naar Gooren, Dik & Stravers (1990). *Registraties geregistreerd II*.
3. 'Over de beweerde onbruikbaarheid van het sofi-nummer voor de zorgsector'. In: *Automatisering Gids*, 7 december 2001; Nouwt, 'Sofi-nummer' 2002, nr. 1, pp. 3-4 en lezing J. Griepink op het Medisch Informatica Congres (MIC), november 2001 in Noordwijkerhout.
4. Sinds 1996 heeft de minister van Binnenlandse Zaken op grond van de paspoortwet de bevoegdheid om paspoorten en andere reisdocumenten aan te wijzen als documenten waarop het sofi-nummer moet worden afgedrukt.
5. Thaens, Zouridis, & Kielema (2002), p. 32 met verwijzing naar Stanley, J. & B. Steinhardt (2002). *Drawing a Blank: The failure of facial recognition technology in Tampa, Florida*. An ACLU Special Report, January.
6. Smin, Hamstra & Van Dijk (1999). *Privacybeleving van burgers*; Koops & Vedder (2001). *Opsporing versus privacy*; Koops & Vedder (2002). 'Particuliere opsporing', pp. 156-165.
7. Tijdens de workshop die voor deze publicatie is gehouden, hebben de deelnemers hun invulling aan de drie begrippen weergegeven. De uitkomsten wezen in dezelfde richting: er bestaat geen eenstemmigheid over de inhoud en betekenis ervan.
8. Hes, Hooghiemstra & Borking (1999). *At face value*, Registratiekamer, via http://www.cbpweb.nl/documenten/av_15_at_face_value.htm

Summary

We are on the eve of important decisions on the creation of a digital identification system. Such fundamental decisions that representatives of the people will have to deal with this subject for years to come. This publication seeks to give Parliament a clearer picture of the:

- issues surrounding digital identification;
- relevant policy initiatives, their context and objectives, also in light of the current political ambitions;
- choices that we face and the possible lines of onward development.

The importance of identification

Personal identification is an important foundation of our society. It allows us to create a link between people, actions and responsibilities. Day-to-day situations requiring some form of identification are numerous and include contacts between private individuals, companies and government. In many ways identification can be seen as one of the 'lubricants' which allow society to function. The government has created an identification system to ensure a smooth social operating process. Physical means of identification (primarily paper identity documents) still predominate.

However, today's information society requires digital equivalents to these physical forms of identification. Without a proper functioning system of digital identification - fighting crime will be seriously obstructed, ambitions in the field of electronic government will be frustrated, companies and citizens will lack faith in *e-commerce* activities, and the national competitive position will ultimately deteriorate, to name but some examples. Careful thinking about the design of a digital identification system is therefore essential.

For government, digital identification is an important linking factor to allow measures to be taken in the field of security, aliens policy, government services and the efficiency of government operations. Digital identification will again play a prominent role on the policy agenda in the coming period. The government which took office in 2003 is expected to continue on the current course, although the discussion has become very one-sided. The current debate on the role of identification pertains essentially to security and aliens policy.

Trends

An overview of the most important European and Dutch policy initiatives in which identification plays a role shows a number of clear trends, social characteristics and points of significance:

- there is enormous confusion as to use of terminology: terminology in the different policy documents is inconsistent;
- there is over-concentration on the physical means: there is hardly attention being paid to the processes involved in the (management of) the identification process;
- the experiments with smartcards have had limited success and will not be integrated for the time being;
- the use of biometrics features for identification purposes is increasing;
- the use of numbers is also increasing, although this is not based on a unequivocal system;
- the same numbers are being used for multiple purposes (multi-chain use);
- the government's monopoly on the allocation of means of identification is faltering;
- the means of identification are increasingly being geared to the individual creating an almost comprehensive picture of a person's identity.

What do these trends mean? What fundamental questions arise? Which direction should be taken in the coming years? The observed trends here lead to four fundamental questions:

1. The infrastructure: unity versus diversity

There is a need for possibilities to coordinate different initiatives and where possible to gear them to each other or integrate them. The most extreme variant of integration is a uniform system for digital identification. However, each step which the government makes in that direction makes society more dependent on the proper functioning of that system and makes citizens more vulnerable.

2. The level of precision: absolute or relative

A second consideration is the question of how precise the means of identification should be. Does the importance of 100% certainty weigh up against the sacrifices (privacy, cost, effort) which citizens will have to accept?

3. Management: public versus private

Who should take the initiative for and the direction and management of the design of digital identification? Where and under what circumstances should government have the monopoly and where could or (even *should*) it leave room for market players? Which sectors should this apply to? Who should set the standards? In which areas should government take action and in which should it not?

4. The wish: convenience and effectiveness versus personal freedom

Over past years developments in the field of information and communication technology have simplified the functioning of society in many ways. The public sector has benefited hugely from ICT. The consequence of these developments could be that government has – or thinks it has – a practically complete picture of its citizens' doings. Based on the supposition that all this information is correct, and using this far-reaching form of identification, government offers the assurance that procedures will be handled more efficiently and rapidly. The question remains to what extent citizens will accept this system improvement under the pretext of convenience. Where should government draw the line and where should it leave the initiative and direction to its citizens?

Recommendations

The mentioned issues are complex and the choices to be made are strongly inter-related. Nevertheless this publication offers a number of recommendations on future policy regarding personal digital identification. Not taking action is not an option, because this will lead to social and economic loss on a macro level.

- 1. It will be advisable for the government to further research citizens' views with regard to digital identification. At this point not enough attention has been paid in the debate to the interests of citizens.*
- 2. Furthermore it should initiate and structure an integral debate that crosses all sector barriers. Four important points in this debate will be:*
 - the focus on long-term developments;*
 - looking beyond the focus on means of identification;*
 - openness to the general public;*
 - target a policy viewpoint with broad consensus to initiate action.*

Also necessary:

- 1. The creation of a system brings with it numerous vulnerabilities, which will require a complex system of checks and balances: a kind of digital precautionary principle, linked to a high measure of legal precision.*
- 2. Furthermore a structure for coordination is needed: there are many conflicts of interest and a wide range of participants will sit at the policy table.*
- 3. Although the creation and management of a digital identification system is a public item, some form a public-private collaboration in the field is not unimaginable. Consideration will have to be given to those areas where learning can be achieved through co-operation, where government should give business free rein, and where government should keep full control.*

Literatuur

Arkel, J. van et al. (1990). 'Verslag van een onderzoek naar persoonsregistraties bij overheid en semi-overheid'. Tilburg: IVA/Voorlopige Raad voor de Persoonsinformatievoorziening.

Cf. (2001). 'Biometrische handtekening'. In: *Privacy & Informatie*, nr. 3.

Gooren, W.A.J. & J.M.A. Schalk (1988). *Registraties geregistreerd. Verslag van een onderzoek naar persoonsregistraties bij overheid en semi-overheid*. Tilburg: IVA/Voorlopige Raad voor de Persoonsinformatievoorziening.

Gooren, W.J.A., J. Dik & F. Stravers, (1990). *Registraties geregistreerd II. Verslag van een vervolgonderzoek naar persoonsregistraties in de openbare sector*. Tilburg: IVA/Voorlopige Raad voor de Persoonsinformatievoorziening.

Grijpink, J. (2002). 'Persoonsnummers en privacy'. In: *Privacy & Informatie*, nr. 2.

Hes, R, T.F.M. Hooghiemstra & J.J. Borking (1999). *At face value. On biometrical identification and privacy* (deel 15 in de serie Achtergrondstudies en Verkenningen). Z.pl.: College bescherming persoonsgegevens.

Koops, B.J. (2001). 'Een nieuwe GBA, digitale kluisjes en identificatiedrang'. In: *Nederlands Juristenblad* afl. 32, pp. 1555-1561.

Koops, B.J. & A. Vedder (2001). *Opsporing versus privacy: de beleving van de burgers*. Den Haag: Sdu Uitgevers.

Koops, B.J. & A. Vedder (2002). 'Particuliere opsporing in de ogen van burgers'. In: *Panopticon*, nr. 2, pp. 156-165.

Nouwt, Sj. (2002). 'Sofi-nummer onbruikbaar in de zorgsector'. In: *Jaarnaal Privacy Gezondheidszorg*, nr. 1, pp. 3-4.

Smink, G.C.J., A.M. Hamstra & H.M.L. van Dijk (1999). *Privacybeleving van burgers in de informatiemaatschappij*. Den Haag: Rathenau Instituut.

Thaens, M., S. Zouridis & J. Kielema (2002). 'Drawing a Blank. The failure of facial recognition technology in Tampa, Florida'. In: *ACLU Special Report*, January.

Internet bronnen

<http://www.consumer.gov/idtheft/reports/gao-d02766.pdf>
http://www.cbpreweb.nl/documenten/av_15_at_face_value.htm
<ftp://ftp.cordis.lu/pub/focus/docs/191en.pdf>

Ministeries

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Projecten Stroomlijning basisgegevens
<http://www.stroomlijningbasisgegevens.nl/projecten/bel.shtml>

Digitaal kluisje
<http://www.gba.nl/documentatie.htm>

Haalbaarheidsstudie biometrie in reisdocumenten
<http://www.bprbzk.nl/downloads/020703.Brief%20TK%20biometrie.pdf>

Nieuwe generatie reisdocumenten
<http://www.bprbzk.nl/>

PKIoverheid
<http://www.pkioverheid.nl>

Overheidsloket 2000
<http://www.ol2000.nl>

Modernisering GBA
<http://www.bprbzk.nl>

Ministerie van Sociale Zaken en Werkgelegenheid

Routerings Instituut Nationale Informatie Stroom (RINIS)
<http://www.rinis.nl>

Ministerie van Volksgezondheid, Welzijn en Sport

Elektronisch patiëntendossier (EPD)

<http://www.minvws.nl/document.html?folder=393&page=13805>

Parkinson-pas

<http://www.npcfcurcus.nl/congres/ICTNaastJeBed.htm>

Ministerie van Verkeer en Waterstaat

Chauffeurspas voor taxichauffeurs

http://www.taxiwet.nl/download/wet_persvervoer_samenv.pdf

Elektronisch autokenteken

http://www.rdw.nl/_jaarverslag2001/jv2001-331.htm

Ministerie van Justitie

Wettelijke identificatieplicht

http://www.justitie.nl/nieuws/080302pmbeperkte_uitbreiding_identificatieplicht.asp

Previumpas Schiphol

<http://nieuws.surfnet.nl/nieuws/hsw/jg01-02/11.html>

Ministerie van Economische Zaken

Overheidsformulieren online

<http://www.minez.nl/ondernemers/online.htm>

Europese Unie

<ftp://ftp.cordis.lu/pub/focus/docs/191en.pdf>

Europese gezondheidskaart

<http://www.emanet.org/Pages/Dutch/ShortAbout.htm>

Europese raadpleging digitale identiteit

<http://www.cordis.lu/spain>

Staatsblad

Wijziging van de paspoortwet
www.recht.nl/index.html?nid=4945

Wijziging regeling DNA-onderzoek in strafzaken
www.recht.nl/index.html?nid=9645

Wet onderwijsnummer
www.onderwijsnummer.nl

EG-richtlijnen

Richtlijn elektronische handel
www.recht.nl/index.html?nid=2880

Richtlijn elektronische handtekening
http://europa.eu.int/ISPO/ecommerce/legal/documents/1999_93/1999_93_nl.pdf