Technologie & Samenleving

Eindredactie

Teksten

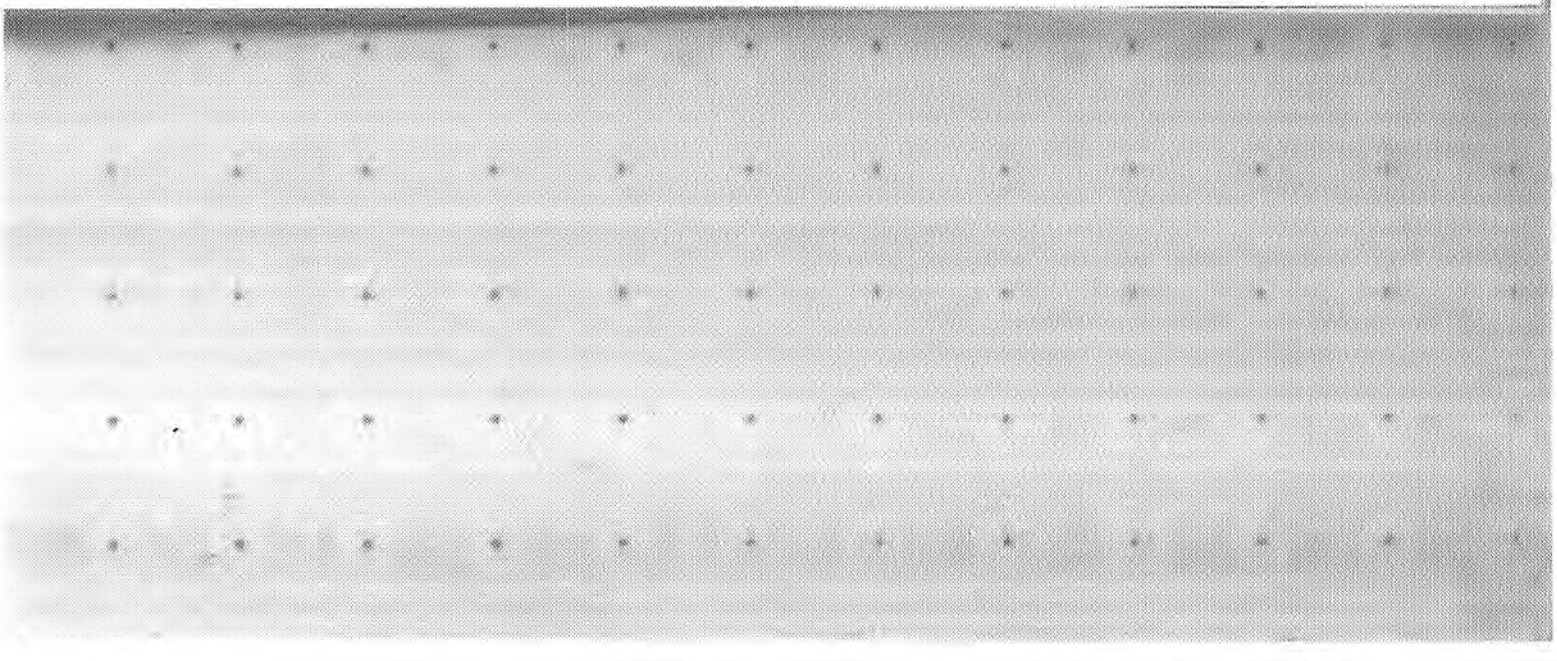
Fotografie

Realisatie

Criminaliteitspreventie

Overheid, burger en biometrie

Den Haag, november 1998



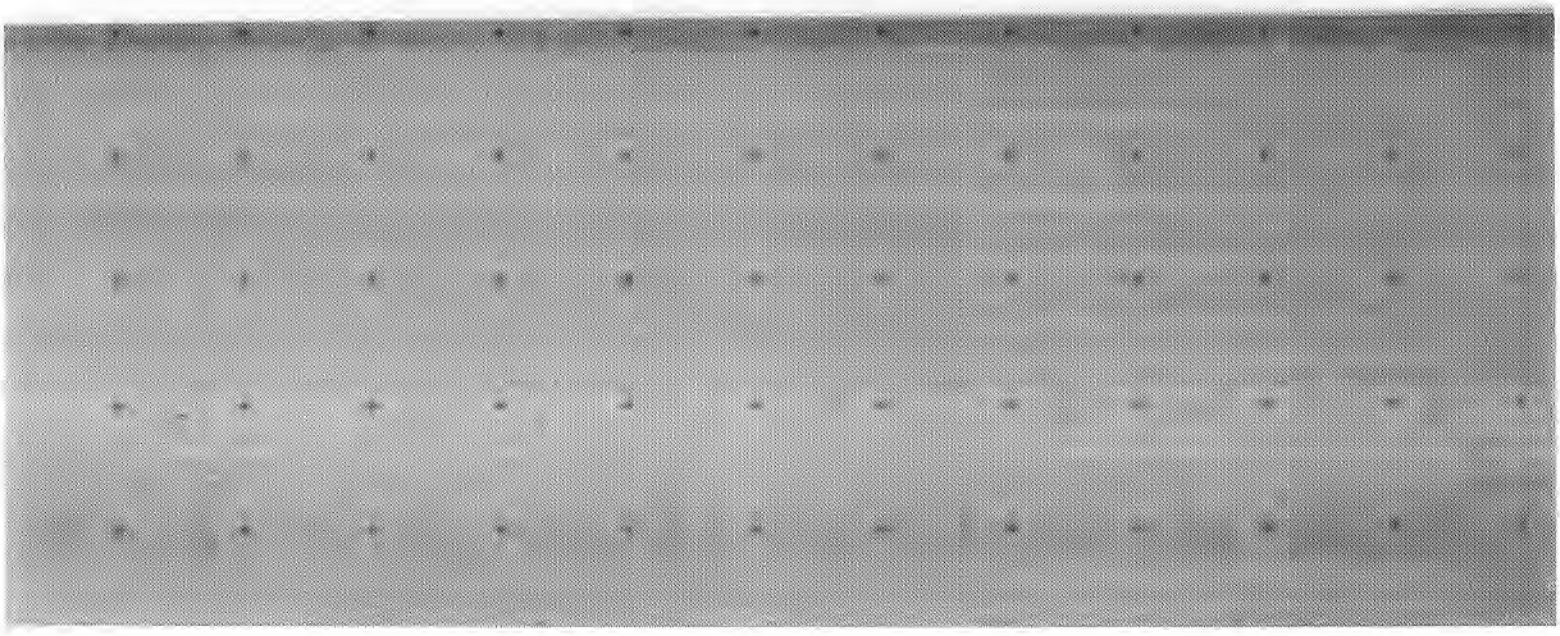
Voorwoord

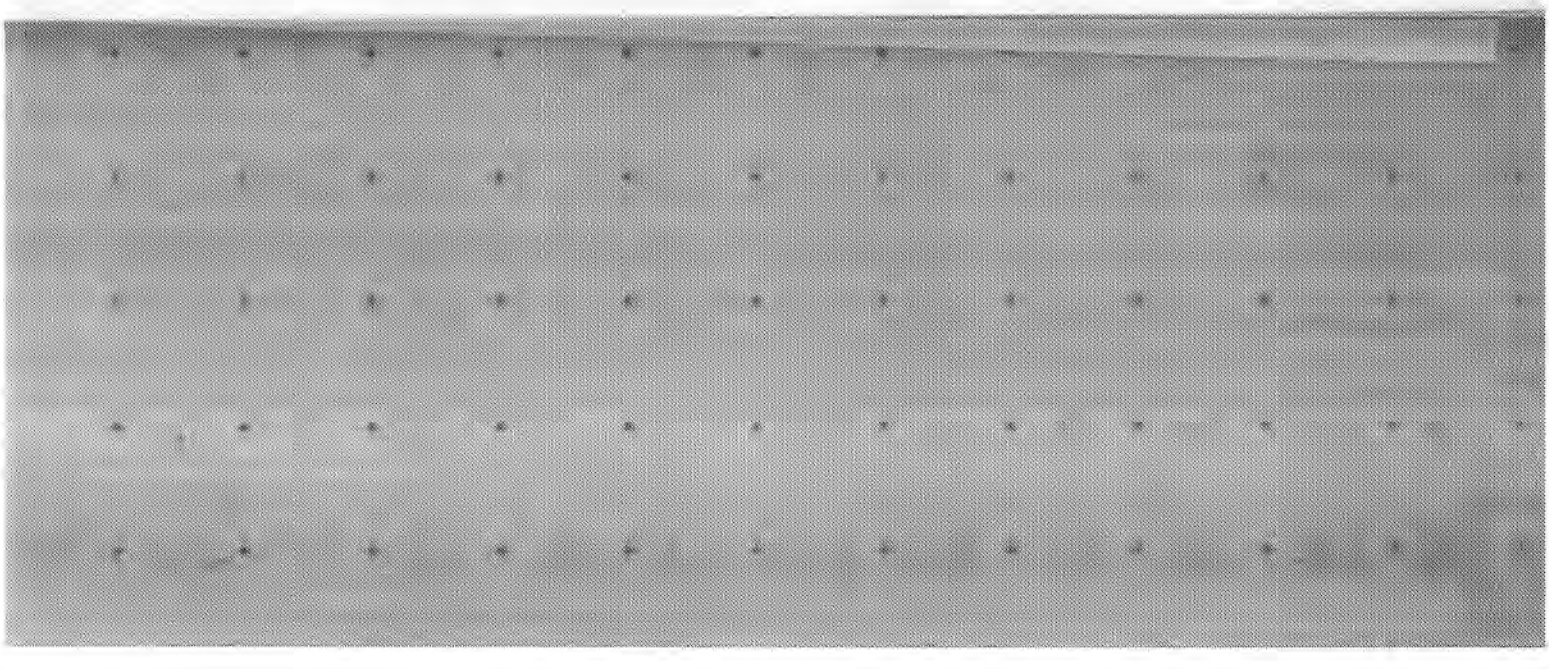
Identificatie is onlosmakelijk verbonden met het functioneren in onze maatschappij. Traditioneel gebeurde dit veelal op basis van een papieren document met een foto zoals het paspoort of het rijbewijs. Ook allerlei organisaties, zoals bijvoorbeeld banken en ziektekostenverzekeraars, maar ook verenigingen, winkels, benzinepompen, gaven en geven in toenemende mate hun eigen 'identificatie-papieren' uit. Meer en meer werd hierbij gebruik gemaakt van een formaat dat we aanduiden met 'pasje': eerst in de vorm van een papieren pasje, maar tegenwoordig vrijwel altijd als plastic pasje. Voor zover er behoefte was aan verificatie – veelal was enkel het in bezit hebben van een pasje al voldoende – gebeurde dit op basis van gezichtsherkenning, de foto uit het paspoort of rijbewijs of de handtekening, zoals bij bank/giropasjes of de creditcard.

De afgelopen periode is er een toename van elektronische identificatie die begon met een magneetstrip, maar tegenwoordig vrijwel altijd de vorm heeft van een chipkaart. Maar ook elektronische identificatie zonder pasjes komt meer en meer voor, zoals bijvoorbeeld bij het inloggen in computersystemen. Met de komst van elektronische identificatie ontstond ook de behoefte aan elektronische verificatie en deden wachtwoorden en pincodes haar intrede. Op het moment is het in bezit hebben van tientallen pasjes en vele pincodes eerder regel dan uitzondering.

Een recente ontwikkeling is het gebruik van biometrie voor identificatie, waarbij gebruik wordt gemaakt van menselijke kenmerken zoals vingerafdruk, handafdruk, de stem, etc. Technologisch zijn er inmiddels vele tientallen systemen die gebruik maken van biometrie. Van een brede toepassing van biometrie is echter nog geen sprake. Hiervoor is er nog veel onduidelijk en ontbreekt de nodige ervaring. In het kader van het stimuleringsprogramma T&S Criminaliteitspreventie zijn er middelen beschikbaar gesteld voor een pilot waarbij met name aandacht zal worden geschonken aan de maatschappelijke acceptatie van biometrie gekoppeld aan een criminaliteitspreventie-toepassing.

Deze publicatie vormt het algemene deel van het werkplan voor deze pilot en beschrijft het kader met betrekking tot de aspecten die een rol spelen bij het toepassen van biometrie. Aanvullend aan deze publicatie is er een specifieke beschrijving van de pilot waarin concreet wordt uitgewerkt welke keuzes er gemaakt zijn voor de pilot en hoe de pilot vorm wordt gegeven.



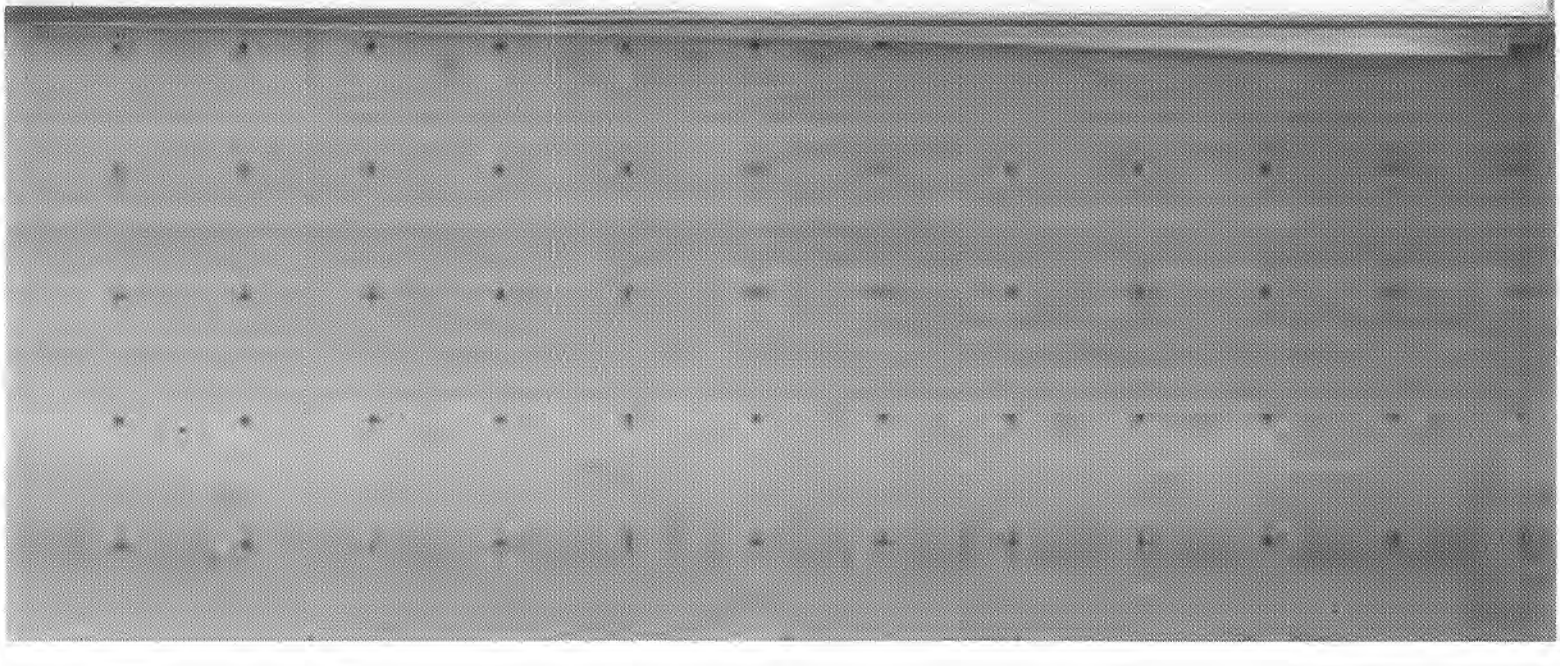


Inleiding

Veel rapporten beginnen de laatste jaren met de zin: *'de technische ontwikkelingen op het gebied van hardware, software en technische infrastructuur zijn dit decennium snel gegaan'*. Het vervolg zou moeten zijn: *'...maar het grootste deel van de burgers blijkt hier amper gebruik van te maken'*. Helaas ontbreekt deze zin vaak.
Deze brochure wil er niet voor pleiten om de burgers koste wat het kost gebruik te laten maken van nieuwe ontwikkelingen rond informatie- en communicatietechnologie (ICT).
Doel is vooral om inzicht te geven in nieuwe technologische mogelijkheden die kunnen bevorderen dat burgers feitelijk gaan profiteren van dergelijke ontwikkelingen. Randvoorwaarde is echter wel dat deze nieuwe diensten en services zich kenmerken door: *'Gewin, Gemak, Genot'*.

Koppeling en integratie van internettechnologie en chipkaarttechnologie (voorname componenten van de informatie- en communicatietechnologie) maken nieuwe vormen van communiceren en informeren mogelijk.
Dit zal mensen beter in staat stellen zich zelfstandig beter te handhaven in de complexe en geïndividualiseerde samenleving van vandaag. Echter de technische mogelijkheden en de wensen van aanbieders van diensten, producten, informatie en infrastructuren bepalen nu de ontwikkeling; en niet de wensen van de afnemers.
Burgers gaan ook niet spontaan op zoek naar dergelijke nieuwe technologische mogelijkheden. De nieuwe technologie dreigt hierdoor onvoldoende aan te sluiten op de wensen en de mogelijkheden van de mensen die haar moeten gebruiken.
Dit raakt ook de kern van de discussie: de burger ziet in het huidige aanbod aan informatie- en communicatietechnologie nog te weinig voordelen. De geboden diensten en services bieden veelal te weinig toegevoegde waarde of hij kan deze ook op een andere – traditionele – manier verkrijgen. De voornaamste reden daarvoor is, dat de nadruk bij de informatie- en communicatietechnologie nog steeds vooral ligt op de techniek en de infrastructuur, niet op de inhoud. Dat is ook voor de producenten en aanbieders een slechte zaak. Het nut voor de burger moet in ieders belang een grotere rol gaan spelen bij de ontwikkelingen.

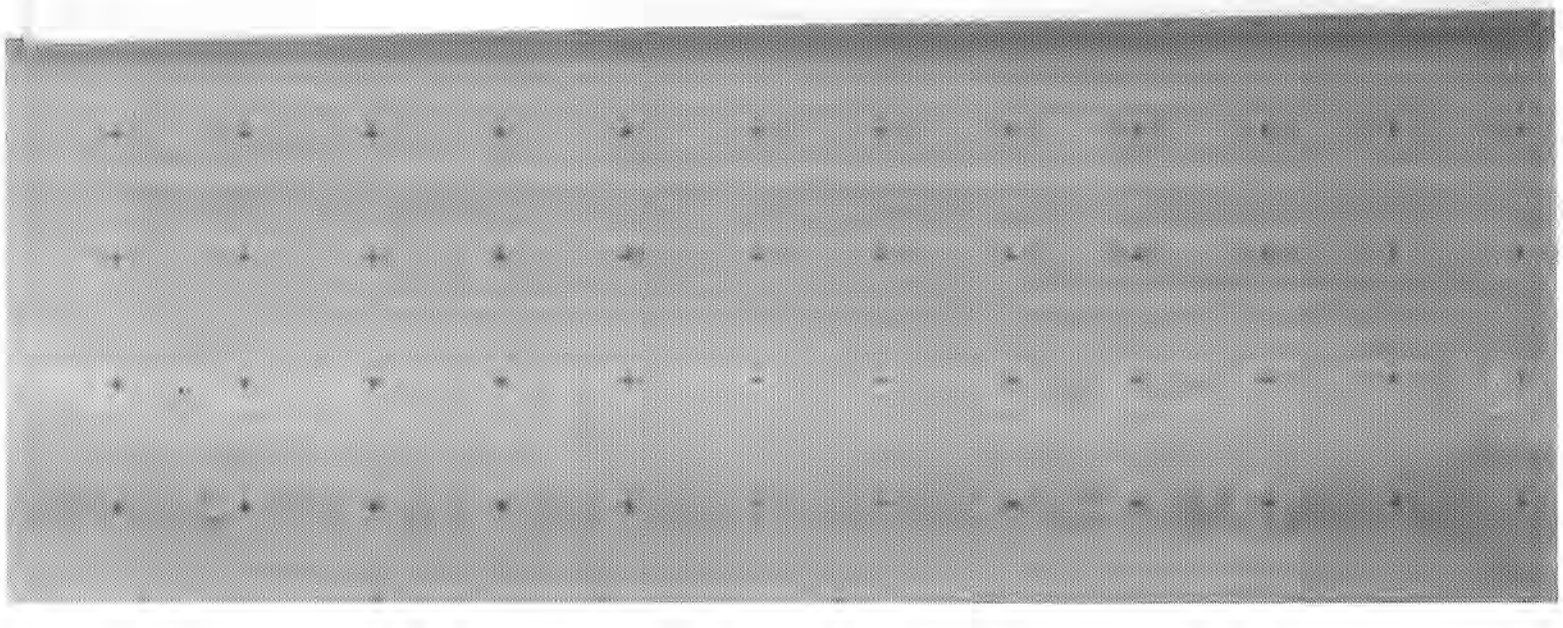
Biometrie is zo'n nieuwe technologie. Deze publicatie richt zich op de mogelijkheden die biometrie biedt voor de overheid. Specifiek wordt ingegaan op de Gemeentelijke dienstverlening naar de burger, waarbij ook aandacht zal worden geschonken aan ontwikkelingen rond de Burger Service Kaart. In algemene zin zal de technologie en het proces rond biometrie worden beschreven, waarbij



ook aandacht worden geschonken aan maatschappelijke acceptatie, kosten-, gebruiks- en risico-aspecten.
De publicatie richt zich echter niet diepgaand op de technische of gebruiksvoor- en nadelen van verschillende vormen van biometrie en/of de juridische overwegingen en/of complicaties rond biometrie.
Het doel is wel dat inzicht wordt gegeven in de toepassing van biometrie die voor de burger het nodige Gewin, Gemak of Genot kan opleveren.

In hoofdstuk 2 wordt een kader geschetst waarin de toepassing van biometrie wordt geplaatst vanuit een overheidsperspectief.
In hoofdstuk 3 wordt ingegaan op de technologische aspecten van biometrie.
Hoofdstuk 4 gaat vervolgens in op de aspecten die bij het toepassen van biometrie een rol spelen.
Tot slot wordt in hoofdstuk 5 een schets gegeven van de te verwachten ontwikkelingen in de nabije toekomst. Hierbij wordt ook ingegaan op het pilotproject dat in Haarlem zal worden uitgevoerd in het kader van de Burger Service Kaart en het deelprogramma Criminaliteitspreventie van de stimuleringsregeling Technologie & Samenleving.

Achterin de publicatie wordt bij de achtergrondinformatie een korte beschrijving gegeven van het NCP en Acquest die deze publicatie hebben samengesteld, het stimuleringsprogramma Technologie & Samenleving en van Senter, de organisatie die belast is met de uitvoering van dit stimuleringsprogramma.



Biometrie: de toepassing

Overheid, burger en biometrie **Criminaliteitspreventie**

Elektronische communicatie tussen overheid en burger gaat een grote vlucht nemen. Naarmate netwerkinfrastructuren zoals internet, intranetten en extranetten breed beschikbaar komen, komen er ook steeds meer mogelijkheden, zodat elektronische overheidsdiensten vanaf iedere willekeurige plek met een netwerkaansluiting kunnen worden afgenomen. De burger/klant vervoegt zich dan niet meer fysiek aan de balie van de overheid, maar logt in op de site van de betreffende overheidsinstantie.

In deze virtuele omgeving wordt het verifiëren van de identiteit van de klant voor de overheid van toenemend belang. Immers naast algemene, voor een breed publiek bedoelde diensten (zoals overheidsinstanties die informatie voor een ieder leesbaar op een website plaatsen) zijn er gegevens en diensten die de overheid alleen en uitsluitend aan de rechthebbende wenst te verstrekken. De overheid wenst daarom, alvorens een bepaalde dienst te verlenen, de identiteit van de burger/klant te verifiëren.

Voor deze verificatie van de identiteit van de burger/klant komen eveneens nieuwe technieken beschikbaar. Van oudsher kennen wij in dat vlak zaken als wachtwoorden en pincodes. Nieuwe mogelijkheden worden geboden door de digitale of elektronische handtekening. Maar ook biometrie als een techniek op basis van bepaalde gedrags- of fysieke kenmerken van de mens, is beschikbaar om de identiteit van een persoon te kunnen verifiëren.

Biometrie en overheid

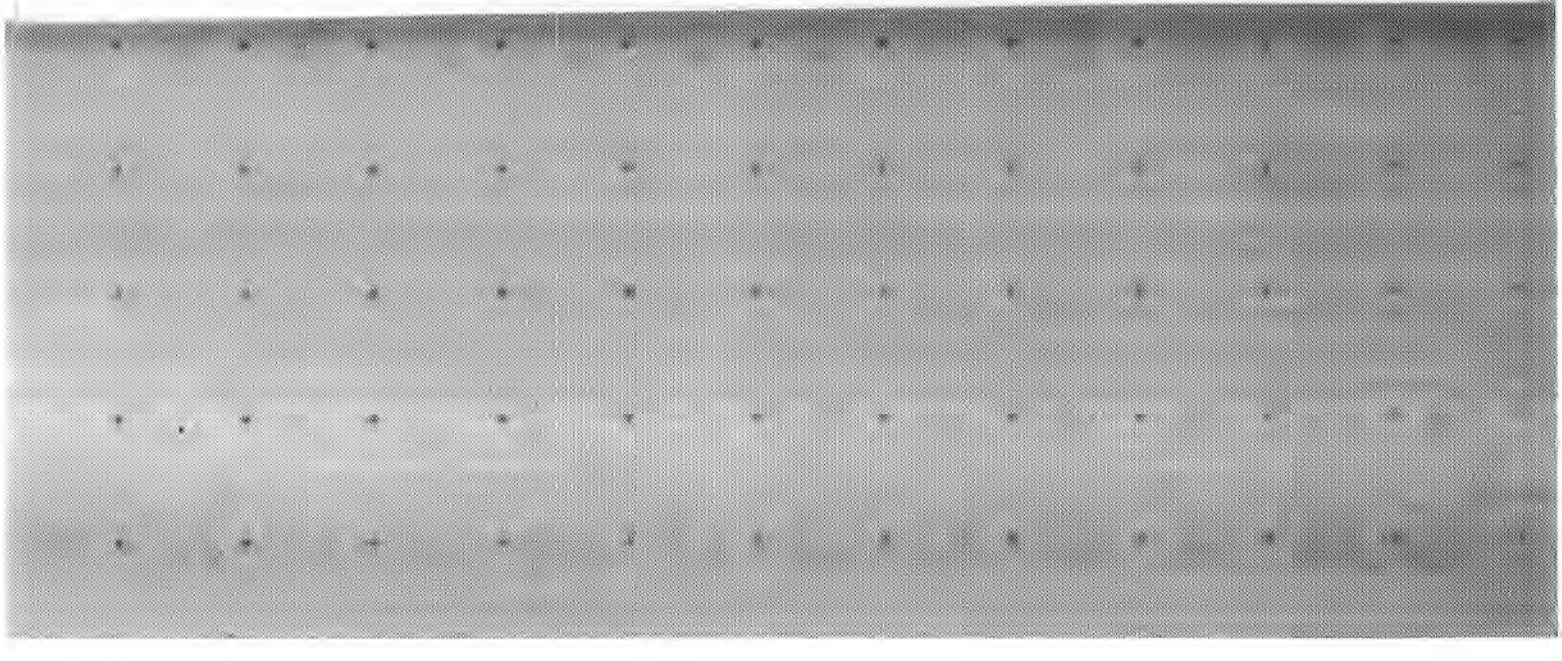
In het Openbaar Bestuur is de Gemeente de instantie die het dichtst bij de burger staat. Veel van de publieke en private Gemeentelijke diensten en activiteiten zijn direct op de inwoners van de Gemeente gericht. Het gaat daarbij om diensten waarbij de burger een gemeentelijk product afneemt (zoals een paspoort, een bouwvergunning, een sociale zekerheidsuitkering) en om diensten waarbij de burger zijn burgerrechten uitoefent (bijvoorbeeld stemmen, gebruik maken van klachtrecht, inzien van bestanden etc.). De laatste decennia is het takenpakket van de Gemeente niet alleen in omvang en intensiteit toegenomen, maar is ook de burger mondiger geworden. Bovendien streeft de Gemeente permanent naar een verbetering van de kwaliteit en de efficiency van haar dienstverlening.

De overheid wil biometrie vaker gaan toepassen, bijvoorbeeld in de dienstverlening. Zo overweegt het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties op termijn biometrie in te zetten bij de nieuwe generatie Europese Identiteitskaarten, de vroegere toeristenkaart. De Gemeenten willen biometrische verificatie inzetten bij bijvoorbeeld:

- toegang tot Gemeentelijke bestanden
- inspraak, referenda, lokaal kiesrecht
- afnemen van diensten van de Gemeentelijke kredietbank
- controle op de fysieke toegang tot onderwijsvoorzieningen.

In het rapport 'Functionele specificaties Burger Service Kaart' van april 1998 zijn tweehonderd Gemeentelijke diensten geschetst waarbij een Burger Service Kaart ondersteunend zou kunnen werken. Een Burger Service Kaart is in deze context een chipkaart, waarop zowel persoonsgegevens van de burger zijn opgenomen (identiteitsfunctie) als waaraan een aantal Gemeentelijke diensten zijn verbonden.

Uiteraard kan de behoefte en keuze om zekerheid te hebben omtrent de identiteit van een persoon, per gemeentelijke dienst sterk uiteenlopen. Redenen hiervoor kunnen



liggen in de sfeer van verbetering van de dienstverlening, maar ook in de sfeer van de fraudebestrijding en criminaliteitsbestrijding. Voor sommige diensten is die wens groot, zoals bij een uitkeringsinstantie. Bij andere diensten is minder zekerheid nodig, bijvoorbeeld bij een toegangsbewijs voor het Gemeentelijke zwembad.

De publieke vs. de private taak van de overheid

Nut en noodzaak van identificatie en verificatie van de burger/klant is zowel voor de centrale overheid als voor de gemeenten van belang. Het maakt immers weinig verschil of iemand uniek geïdentificeerd moet worden door bijvoorbeeld de Belastingdienst (vergelijk de Belasting aangifte diskette met zelfgekozen pincode) of door de Gemeente, bijvoorbeeld bij afgifte van een uittreksel van het bevolkingsregister.

Bij de uitvoering van de identificatie en de verificatie kan het van belang zijn of er sprake is van een publieke taak of een private taak van de overheid. Het betreffen dan veelal taken of diensten waar de overheid een monopolie-positie bij heeft. Soms is in die gevallen bij de wet ook vastgelegd welke identificatie- en verificatiemiddelen daarbij gebruikt dienen te worden. Maar door haar monopolie-positie dient de overheid er ook voor te waken niet onnodig strenge eisen te stellen aan – in dit geval – de methode voor het vaststellen van de identiteit. (In hoofdstuk 3 wordt dit aspect bij het onderwerp proportionaliteit nader uitgewerkt.)

In de private sfeer is de rol van de overheid minder expliciet. De overheid heeft hier meer vrijheid bij de uitvoering van de opgedragen of zelf gekozen taak. Ook betreft het diensten die verzelfstandigd kunnen zijn of uitgevoerd worden door commerciële bedrijven. De rol en de mogelijkheden van de overheid zijn in deze niet anders dan die van elke andere private onderneming of organisatie.

De huidige praktijk van identificatie en verificatie

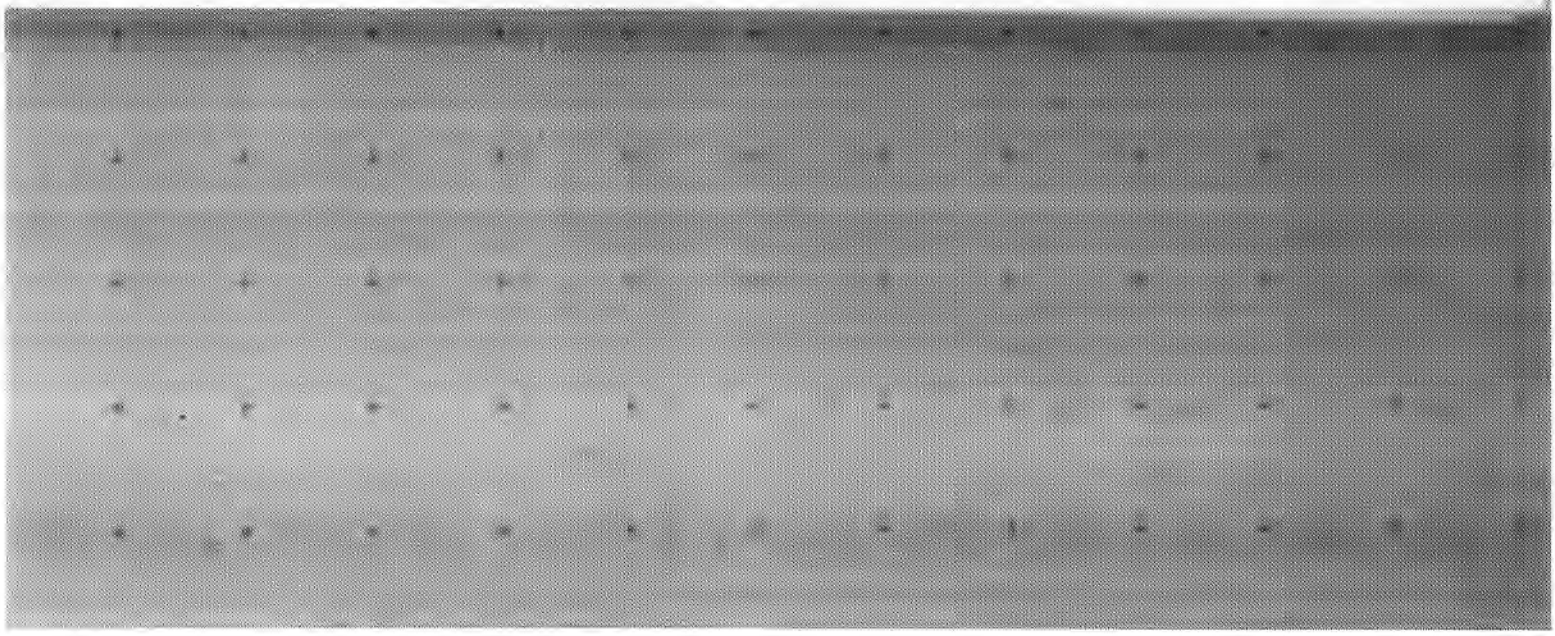
De Gemeente moet bij dienstverlening nagaan, of zij wel te maken heeft met de persoon die recht heeft op deze dienst, dat wil zeggen: of de aanvrager wel de gerechtigde is. Op dit moment kan zij in principe de volgende middelen hanteren om de identiteit te verifiëren:

- iets dat iemand in zijn bezit heeft (meestal een op naam gesteld en persoonsgebonden document)
- iets dat iemand weet (bijvoorbeeld een pincode)
- een handelingskenmerk van een persoon (bijvoorbeeld iemands stem)
- een fysiek kenmerk van een persoon (bijvoorbeeld een fotografische afbeelding of een vingerafdruk).

In de huidige praktijk wordt als beveiligingsmaatregel ter verificatie van de identiteit van een kaarthouder meestal volstaan met een foto (paspoort, rijbewijs), een handtekening (machtiging of verklaring) of een pincode (bankpas). Deze verificatiemethoden kennen alle de nodige zwakten.

Van 'fotoherkenning' is bekend, dat deze door daarvoor opgeleid personeel goed kan worden uitgevoerd, bijvoorbeeld de Koninklijke Marechaussee op de lucht- en zeehavens. Amerikaanse supermarktcaissières bleken een kaart vaak onterecht te accepteren: in 35% van de gevallen waarin iemand een kaart met een foto van een geheel verschillende persoon presenteerde, en in 64% van de gevallen waarin een kaart met een foto van een gelijkende persoon gepresenteerd werd.[1]

Bij creditcardbetalingen moet de handtekening op de kaart met de handtekening op de betaalslip vergeleken worden. Iedereen die in winkels en restaurants regelmatig met een creditcard betaalt, kent de geringe intensiteit waarmee gecontroleerd wordt. Het systeem is daarmee



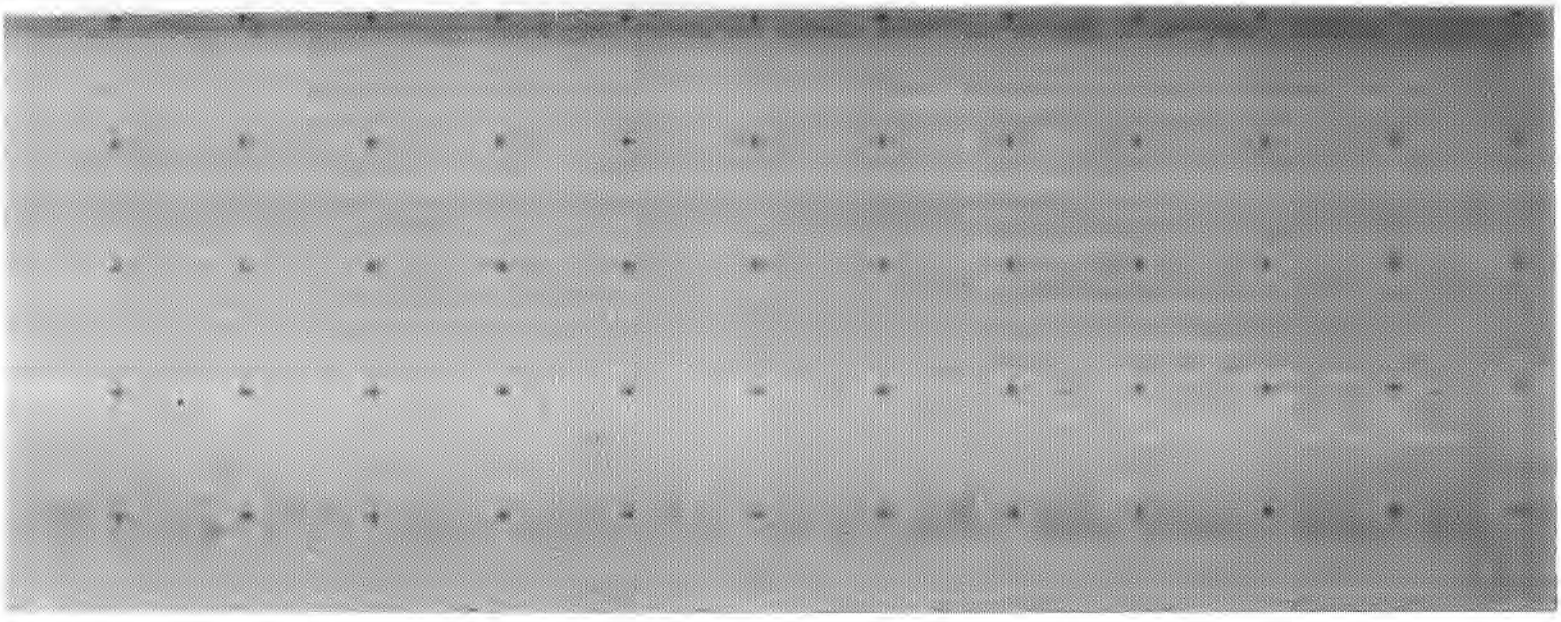
inherent zwak. Het aantal klachten blijft alleen beperkt omdat de creditcardmaatschappijen een zeer soepel beleid voeren en het risico op zich nemen.

Aangezien handmatige controles vaak niet of slecht worden uitgevoerd, is er veel te zeggen voor automatische identificatiemethodes. In ieder geval in die situaties waarin van enige massaliteit sprake is.

Een 100% betrouwbare vergelijking kan bijvoorbeeld met een wachtwoord. Nadeel van deze vorm van verificatie is dat een pincode overdraagbaar is: de code kan aan de kaarthouder worden ontfutseld, of hij of zij kan de pincode aan een andere persoon overdragen. In het meest negatieve geval is hierbij sprake van samenspanning. De Gemeente (of welke andere dienstverlenende organisatie dan ook) kan niet met zekerheid zeggen dat de rechtmatige houder van de pincode de dienst aanvraagt dan wel heeft afgenomen. Een pincode is eerder een negatieve vorm van verificatie: een foutieve pin wijst ondubbelzinnig op onjuist gebruik, maar een correcte pin bewijst niet automatisch rechtmatig gebruik. Er is dus geen sprake van de 'unieke' (onomstotelijke) persoonsidentificatie, die - zoals hiervoor aangegeven - steeds belangrijker zal worden voor betrouwbare dienstverlening.

Een bijkomend probleem van de pincode is de noodzaak om deze te 'onthouden'. Bij een of twee pincodes per persoon, die bovendien regelmatig gebruikt worden (zoals bijvoorbeeld bij het GSM-toestel en de bankpas waarmee regelmatig wordt betaald) levert dit in het algemeen weinig problemen op. Dit wordt anders wanneer de burger over veel meer pincodes gaat beschikken.
De introductie van de elektronische beurs in chipkaartvorm heeft het aantal in gebruik zijnde pincodes in Nederland met bijna 20 miljoen doen toenemen. Al gauw zal het aantal verschillende pincodes dat iedere burger heeft toebedeeld gekregen, dusdanig omvangrijk zijn, dat dit voor de burger onhanteerbaar wordt. Een mogelijke oplossing ligt in het bieden van de keuzemogelijkheid aan de burger/klant om zelf zijn eigen pin(nen) te kiezen.

[1] Onderzoek Westminster University, Postnews Vol 22 no. 1 januari 1996



Biometrie, de technologie

Onder biometrie wordt verstaan een persoonsherkenning of verificatie aan de hand van een uniek lichamelijk kenmerk, waarbij onderscheid wordt gemaakt in:

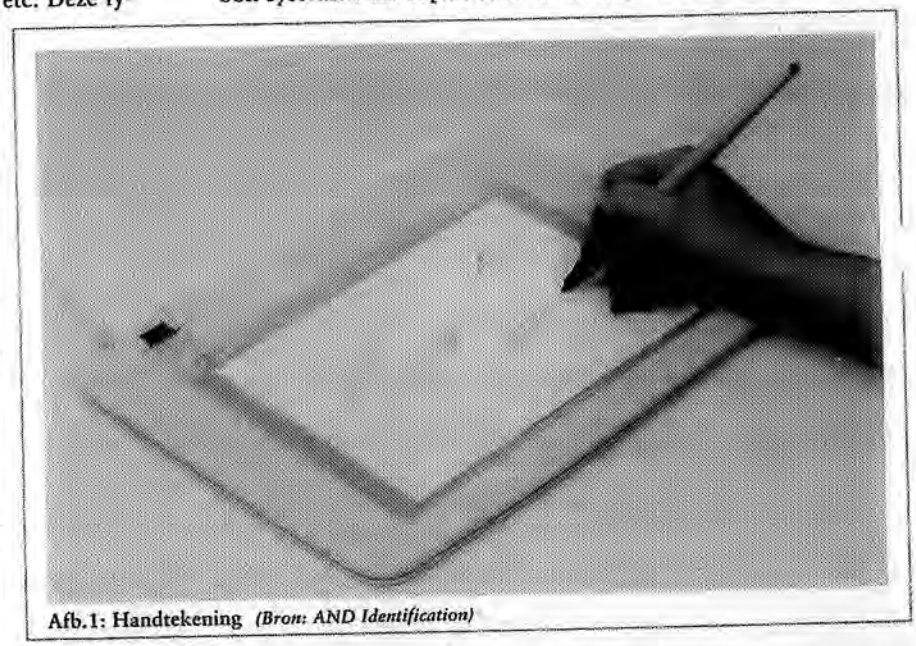
- *Gedragsmatige karakteristieken.* Dit zijn de meetbare aspecten van de manier waarop een persoon handelt of zich uit. Voorbeelden hiervan zijn de stem, de manier waarop iemand een handtekening plaatst en de wijze waarop iemand een toetsenbord bedient. Deze karakteristieken zijn binnen bepaalde bandbreedtes stabiel van aard, maar kunnen over een langere periode (geleidelijk) veranderen.
- *Fysieke karakteristieken.* Dit zijn bepaalde lichaamskenmerken, die normaal gesproken bij ieder persoon aanwezig zijn. Voorbeelden hiervan zijn vingerafdruk, iris- en retinapatroon, gezichtspatroon, warmtepatroon van het gezicht, vorm van het oor, geometrie van de vingers, handpalmpatroon, geurpatronen etc. Deze fysieke karakteristieken zijn in beginsel niet aan verandering onderhevig.

Zoals gezegd zijn de gedragskenmerken in de loop van de tijd aan veranderingen onderhevig. De stem kan 'hoger' of 'lager' worden; of de uitspraak kan langzamerhand veranderen. Ditzelfde geldt voor de handtekening. Door het veelvuldig plaatsen van de handtekening kan de vorm wat gestileerder worden en de snelheid van het 'zetten' van de handtekening toenemen. Wanneer de afwijkingen te groot worden ten opzichte van de oorspronkelijk vastgestelde patronen, dient opnieuw vastlegging van het patroon plaats te vinden Dit vastleggen wordt 'enrollment' genoemd.
Bij fysieke kenmerken is de verandering beduidend minder. Wel kunnen door bepaalde ziekten (bijvoorbeeld aan iris of retina van het oog) vervormingen optreden die buiten de tolerantiegrenzen van het systeem vallen. Enrollment van het gezonde oog is dan noodzakelijk. Omdat fysieke karakteristieken minder gevoelig zijn voor verandering dan gedragskarakteristieken, bieden zij een hoger beveiligingsniveau. De Nederlandse Praktijkrichtlijn voor de Open Infrastructuur voor chipkaarttoepassingen (NPR 7402) spreekt dan ook een voorkeur uit voor toepassing van fysieke karakteristieken.

Technieken bij de gedragskenmerken

Dynamische handtekening (zie afb.1)

In het algemeen gaat het hierbij om de druk en de snelheid waarmee een handtekening wordt gezet. Er zijn ook systemen die bepaalde karakteristieken van de hand-



Afb.1: Handtekening *(Bron: AND Identification)*

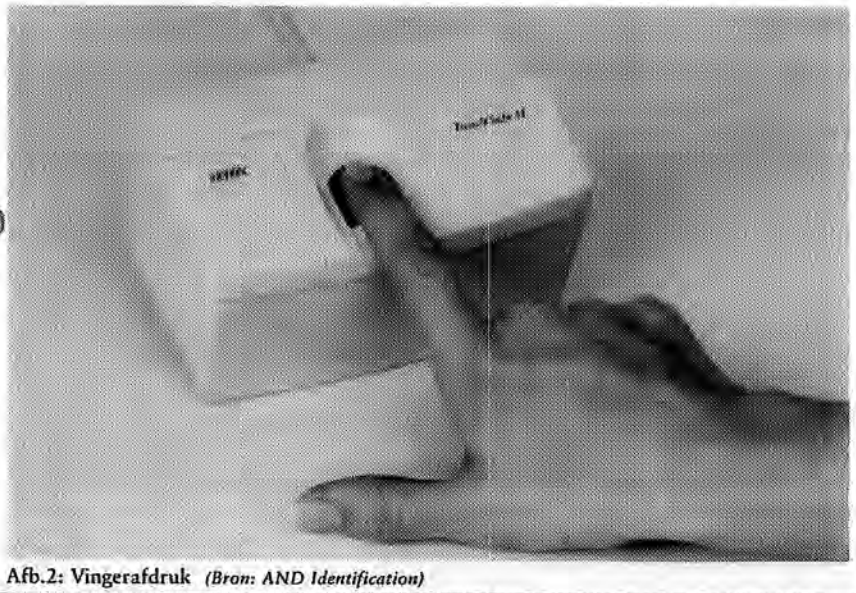
tekening meten, zoals ophalen in de letters etc.
Verder zijn er systemen die met een speciale pen werken, de pen is dan meetinstrument. De handtekening wordt gezet op een z.g. tablet. Hiervoor is al een product op de markt. Een handtekening zetten voor identificatie sluit goed aan bij het huidige maatschappelijk gebruik en is gebruikersvriendelijk. Proefprojecten in Engeland (onder meer bij de uitvoering van de sociale verzekeringsregelgeving) hebben goede resultaten opgeleverd.

Stemherkenning

Systemen voor spraakherkenning, die de semantische betekenis van het gesproken woord herkennen, zijn al in gebruik bij elektronische informatiediensten, besteldiensten en elektronisch bankieren. Via de telefoon is hiervoor een uitgebreid programma beschikbaar. Stemherkenningsystemen voor verificatiedoeleinden kunnen op die toepassing aansluiten. Zulke systemen moeten beschermd worden tegen misbruik via bandopnamen van de betrokken stem. Dergelijke systemen zijn redelijk bestand tegen stemvervormingen door nervositeit, buiten adem zijn en aandoeningen van de luchtwegen. De techniek is zonder meer gebruikersvriendelijk: mensen zijn gewend elkaar aan de stem te herkennen.

Typeaanslag

Ieder mens bedient een toetsenbord op een unieke manier. Zij kunnen daaraan worden herkend, net zoals vroeger radiotelegrafisten aan de wijze waarop zij een morsesleutel bedienden. De techniek lijkt niet erg geschikt voor massale toepassing door de overheid, maar kan wel worden ingezet voor eigen personeel dat een PC met toetsenbord bedient.

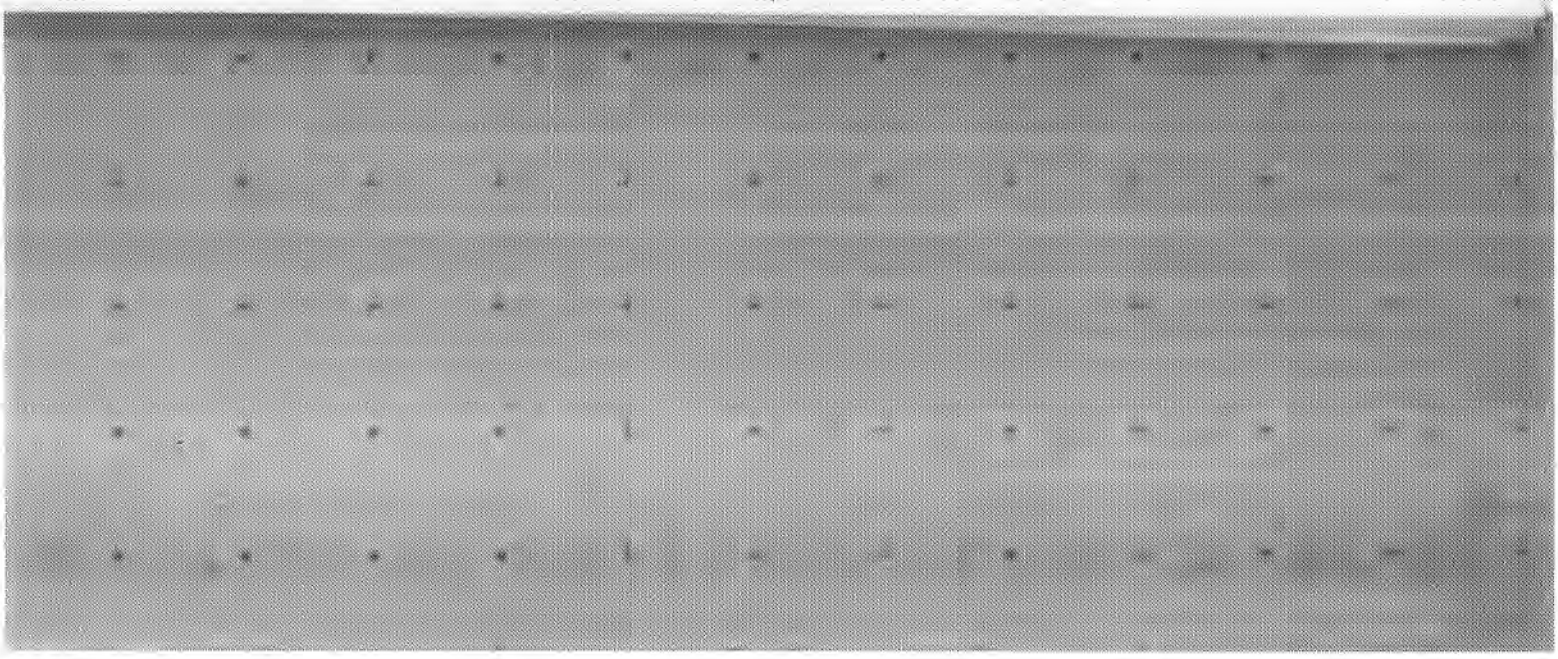


Afb.2: Vingerafdruk *(Bron: AND Identification)*

Technieken bij de fysieke kenmerken

Vingerafdruk (zie afb.2)

De vingerafdruk vormt de 'oudste' en meest bekende van de verschillende technieken. Nehemia Gruw van de Royal Society in Londen ontdekte al in 1684 dat vingerafdrukken verschillend waren en systematisch konden worden geclassificeerd. Zij zijn redelijk constant, maar kunnen wel slijten door bepaalde soorten handarbeid, zoals metselen. Ook bij éénеiige tweelingen zijn vingerafdrukpatronen uniek. Bij vingerafdrukherkenning worden patronen vergeleken van 'minutiae', dit zijn de punten waarop vingerafdruklijnen eindigen, elkaar kruisen of zich



splitsen. Er zijn wereldwijd meer dan 100 leveranciers van vingerafdruksystemen. Vingerafdruklezers kunnen optisch, met ultrasoon geluid of met capacitieve sensoren werken. Technisch is de vingerafdruk de meest uitgekristalliseerde techniek, maar qua maatschappelijke acceptatie scoort zij laag in verband met de associatie met criminaliteitsbestrijding en opsporing.

Handgeometrie (zie afb.3)

Bij deze techniek worden de karakteristieken van de vingers van de hand gemeten. De eerste systemen dateren uit de jaren '70: zij maten de lengte van de vingers. Moderne systemen gaan uit van verschillende karakteristieken van de hand en meten zowel de bovenkant van de hand, de zijkant als soms ook de beenstructuur. De meest gebruikte systemen gaan uit van twee of vijf vingers. Voordeel hiervan is dat de template – na bewerking – erg klein is (9 tot 11 bytes). De Amerikaanse Immigratiedienst experimenteert al sinds langere tijd met handgeometrie.

Handpalmherkenning

Handpalmherkenning werkt ongeveer hetzelfde als de vingerafdruk, het meet de lijnen van de palm van de hand. Een palmafdruk schijnt even uniek te zijn als een vingerafdruk.

Aderpatroon

Dit systeem werkt met de herkenning van het aderpatroon op de rug van de hand.

Retinascan

Van alle biometrische technieken biedt gebruik van het oog de beste beveiliging tegen inbreuk. Tegelijkertijd wordt deze techniek als weinig gebruiksvriendelijk ervaren. Bovendien zijn de systemen vrij kostbaar. Het systeem maakt gebruikt van het feit dat de retina aan de achterzijde van het oog een uniek patroon van bloedvaten heeft. De eerste retinasystemen kwamen beschikbaar in 1985.

Irisscan

Dit systeem gebruikt infrarood licht om een afbeelding van het irispatroon vast te leggen. De gebruiker moet in een camera kijken en zijn oog daarvoor in de goede positie brengen. Een gemiddeld template is 256 bytes.

Oorpatroon

Het oor van ieder mens heeft eveneens unieke karakteristieken. Een van de systemen gebruikt een soort telefoonhoorn waarin een verlichtingselement en een camera zijn ingebouwd. Inmiddels is in een strafzaak een oorafdruk als bewijsmateriaal erkend.

Afb.3: Handafdruk *(Bron: AND Identification)*

Gezichtspatroon

Dit systeem werkt met kleine camera's en algoritmen die karakteristieken van het gezicht berekenen. Moderne systemen gaan er daarbij reeds vanuit dat wat wordt aangeboden een menselijk gezicht is. De systemen registreren de positie van de verschillende kenmerken (ogen, neus, mond), en de onderlinge afstanden van deze kenmerken. De techniek werkt alleen goed bij voldoende lichtcondities. Baarden en brillen kunnen storen. De techniek is gebruiksvriendelijk, mensen vinden het normaal om elkaar visueel te herkennen. Enkele buitenlandse banken experimenteren met deze technologie bij geldautomaten.

Warmtepatroon van het gezicht (zie afb.4)

Dit is een zeer betrouwbare techniek. De verschillende delen van het gezicht hebben verschillende temperaturen. Hiervan kan een soort warmtekaart worden gemaakt,

Afb.4: Gezichtsafdruk *(Bron: AND Identification)*

voor vergelijk met latere opnamen. Ook bij verschillende omgevingstemperaturen blijven de onderlinge temperatuurverhoudingen van de delen van het gezicht gelijk. De apparatuur is echter vrij omvangrijk en nogal duur.

Geurpatroon

Ieder mens heeft een uniek geurpatroon, dat ook na lichamelijke inspanning ongewijzigd schijnt te blijven. Ook zware parfums beïnvloeden het systeem niet. Er zijn nog geen commerciële toepassingen bekend.

Het proces rond biometrie

Voor een goed begrip van de procesgang van identificatie en verificatie bij biometrie is het van belang onderscheid te maken tussen de fase van de eenmalige, eerste vastlegging van de biometrische gegevens in de zogeheten personalisatiefase en de daarna volgende herhaaldelijke verificaties tijdens de gebruiksfase.

Eerste vastlegging of enrollment

Met name de eerste fase van de eenmalige vaststelling van de identiteit en de koppeling van de biometrische gegevens aan de juiste persoon, is een fase die voor de Gemeente van groot belang is. De Gemeente is daarvoor ook als geen andere organisatie toegerust.

De Gemeente gaat bij het uitgeven van Paspoort, Rijbewijs en Europese Identiteitskaart als volgt te werk. Indien het om een eerste afgifte van documenten gaat, kan de Gemeente niet terugvallen op een vergelijking met andere documenten. De Gemeente kan dan de identiteit vaststellen uit eigen wetenschap (bijvoorbeeld omdat de behandelend ambtenaar de burger die het document aanvraagt persoonlijk kent) of door middel van een enquête: de gemeenteambtenaar bevraagt daarbij de document-

aanvrager aan de hand van gegevens die in de Gemeentelijke bevolkingsadministratie zijn vastgelegd. Dat kunnen dan vragen zijn als: op welke adressen heeft u vroeger gewoond, waar en wanneer zijn uw ouders gehuwd, wat is de tweede voornaam van uw grootmoeder etc.
Ook kan de Gemeente als 'aanvullend bewijsmateriaal' op naam gestelde en persoonsgebonden documenten accepteren. Nadat de gemeenteambtenaar de identiteit heeft vastgesteld, worden de administratieve gegevens (naam, geboortedatum, geslacht, nationaliteit etc.) verbonden met de gegevens die later voor verificatie gebruikt worden. Bij Paspoort en Rijbewijs is dat de foto die aan het document wordt gehecht. Aangezien het eindproduct een ingevuld Paspoort of Rijbewijs is, wordt deze fase ook wel aangeduid als 'personalisatiefase'.

Voor toekomstige verificatie slaat de Gemeente een duplo van de foto op het document op in haar administratie. Als de aanvrager een eerder afgegeven document kan overleggen, hoeft de Gemeente de identiteit niet vast te stellen maar kan zij volstaan met het verifiëren van de identiteit, zoals die in het door de burger getoonde document is vastgesteld.

Ook bij toepassing van biometrie identificeert de Gemeente de identiteit van een persoon en legt vervolgens de biometrische karakteristieken in elektronische vorm vast. Zo kan op ieder moment een relatie worden gelegd tussen de administratieve identiteit en het biometrische kenmerk.

Gebruiksfase

In de gebruiksfase vergelijkt een systeem steeds de gemeten biometriewaarde (de zogeheten life template) met de waarde van het tijdens de identiteitsvaststellings- of personalisatiefase vastgelegde kenmerk (de z.g. stored template). Het resultaat van deze vergelijking is een waarschijnlijkheidsscore dat de persoon die de life template aanbiedt, dezelfde is als de persoon waarvan tijdens de fase van de identiteitsvaststelling de stored template is vastgelegd. Het gaat om een waarschijnlijkheidsscore omdat de waarden van twee templates nooit 100% gelijk zijn.

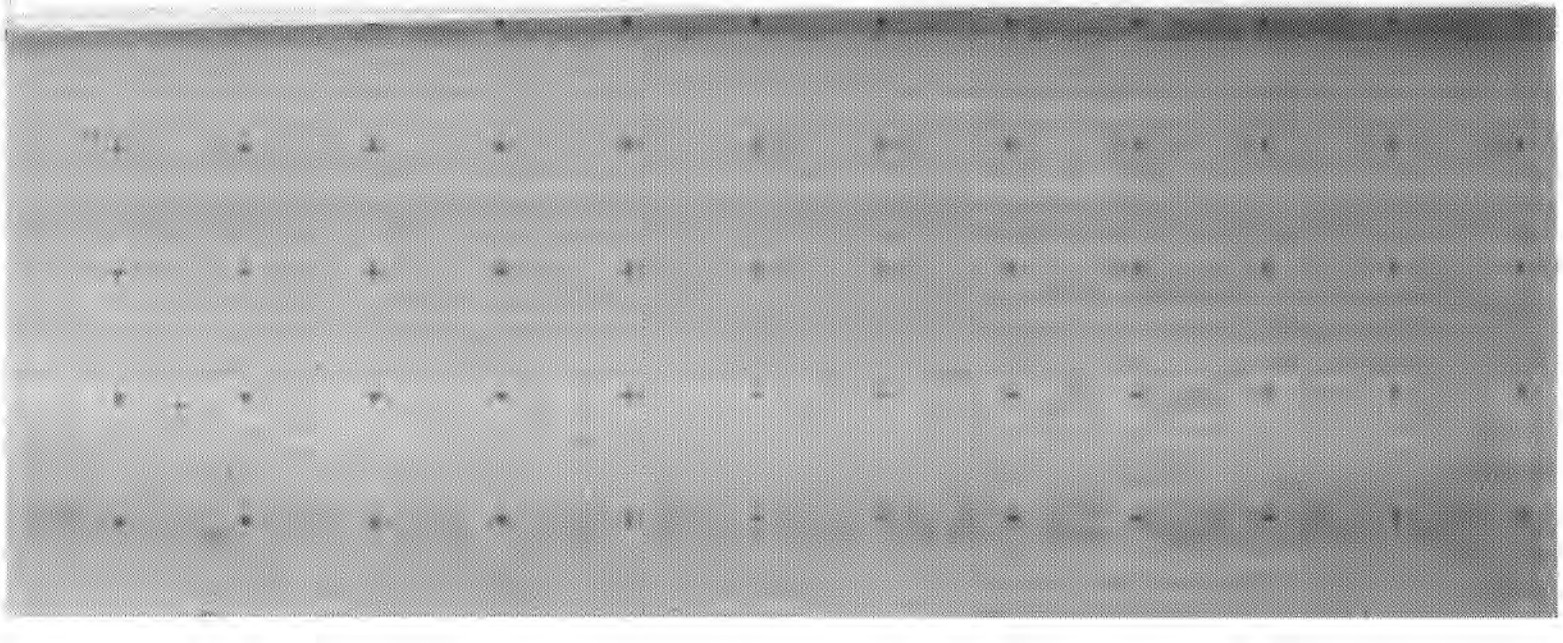
Verschillende niveaus van betrouwbaarheid

Verifiëren van de identiteit van een persoon kan in verschillende maten van betrouwbaarheid. In oplopende volgorde zijn er vijf verschillende betrouwbaarheidsniveaus:

1: verificatie van de administratieve gegevens van een persoon
2: menselijk-visuele verificatie, door vergelijken met een foto
3: verificatie d.m.v. een sleutel, zoals een pincode
4: verificatie d.m.v. een biometrisch gedragskenmerk
5: verificatie d.m.v. een fysiek biometrisch kenmerk

In de huidige maatschappelijke praktijk vindt verificatie vooral plaats op betrouwbaarheidsniveau 1 of 2, met officiële identiteitsbewijzen zoals Paspoort, Rijbewijs en Rijksidentiteitskaart. Betrouwbaarheidsniveau 3 wordt vooral toegepast door de banken, bijvoorbeeld bij de geldautomaat en bij pinbetalingen aan de kassa. Ook bij telebankieren wordt de pin in allerlei vormen toegepast. Biometrie – de hoogste vorm van beveiliging - wordt door overheid en bedrijfsleven nog slechts beperkt toegepast. Het gebruik beperkt zich voornamelijk tot toegangscontrole, bijvoorbeeld in asielzoekerscentra en in penitentiaire inrichtingen.

Een aspect van aandacht is de zogeheten 'identiteits-



lift': als er meer en betere voorzieningen beschikbaar komen om de identiteit van een persoon te verifiëren zal daar ook meer en meer gebruik van worden gemaakt. Oók in situaties waar voor die tijd de noodzaak tot verificatie van de identiteit kennelijk minder werd gevoeld. In die zin is er sprake van een opwaartse druk in het betrouwbaarheidsniveau van verificatie, zeker als zo'n verificatie geautomatiseerd kan worden uitgevoerd.

Een goed voorbeeld in dat verband is de Gemeentelijke Bevolkingsadministratie Persoonsgegevens. Dit bestand is inmiddels in volledig geautomatiseerde vorm beschikbaar en – onder juridische voorwaarden – te raadplegen. Steeds vaker wordt dit bestand geraadpleegd voor actuele informatie, waarmee ook het volume aan verificatieverzoeken sterk is toegenomen. Als de overheid biometrische verificatiemiddelen ontwikkelt, mag ook worden aangenomen dat zowel de overheid zelf als anderen daarvan zeer breed gebruik gaan maken.

In algemene zin, maar zeker voor de overheid in de uitvoering van zowel haar publieke als haar private taak dienen de beginselen van proportionaliteit en subsidiariteit in het oog gehouden te worden. Proportionaliteit wil zeggen dat het middel van identificatie en verificatie in een juiste verhouding dient te staan tot het doel dat de overheid hiermee beoogt te dienen. Wat betreft de subsidiariteit dient de overheid zich steeds af te vragen of niet op een andere, eenvoudiger wijze in de behoefte van geïdentificeerd en of geverifieerd kan worden.

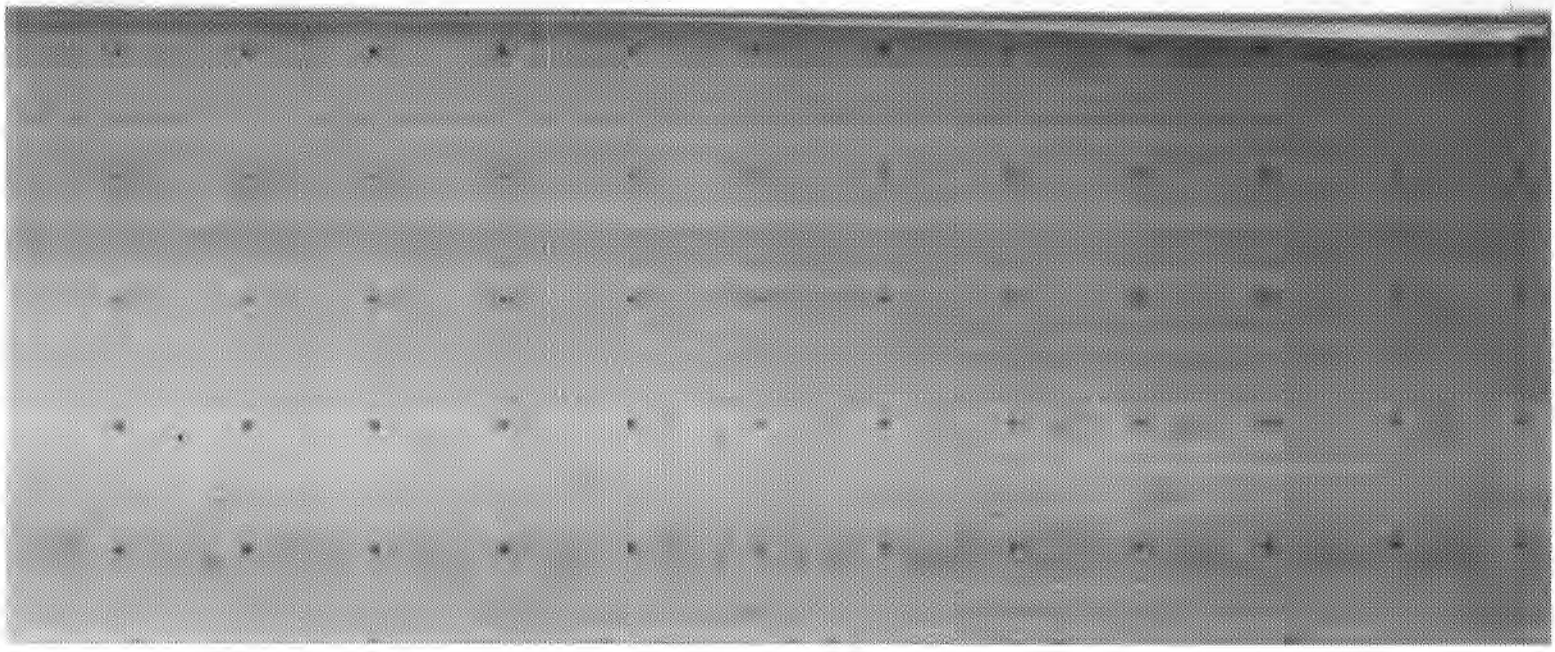
Anonieme biometrie

Het is niet strikt noodzakelijk dat de administratieve persoonsgegevens tijdens het verificatieproces een rol spelen. Die zijn immers al aan de orde geweest bij het vaststellen van de identiteit tijdens het enrollmentproces. In bepaalde situaties, waarin het niet noodzakelijk is de persoon met naam en toenaam te kennen, kan dat bijzondere voordelen bieden omdat zo de privacy van een persoon volledig ongemoeid kan blijven. Het biometrische template van de persoon vormt dan als het ware een soort privacy protector, een 'embleem' dat bepaalde fysieke en elektronische poorten opent waartoe de persoon in kwestie geautoriseerd is, maar zonder dat zijn identiteit in het verificatieproces aan de orde komt.

Neem bijvoorbeeld een toegangssysteem. Stel het biometrisch kenmerk van een persoon zit in het systeem van 'stored templates'. Als de biometrische lezer een life template afleest, die voldoende overeenkomt met een template uit het stored systeem, is de aanbieder blijkbaar gerechtigd naar binnen te gaan. Het systeem opent dus de deur, de toegangsdeur wordt geopend, maar hoeft daarbij niet te weten welke persoon nu precies naar binnen is gegaan. Het enige dat het systeem weet is dat één van de personen die behoort tot de groep van personen die toegangsgerechtigd zijn, de toegangsdeur is gepasseerd.
Deze werkwijze wordt wel aangeduid als 'anonieme' biometrie. Anonieme biometrie kan in principe zowel worden uitgevoerd met een centrale database, een decentrale database als in een systeem waarbij de persoon zelf zijn biometrische template op een of andere informatiedrager (zoals een chipkaart) bij zich draagt.

Biometrie en chipkaart

Zoals aangegeven in de inleiding, vormt de chipkaart, naast Internet en biometrie, een interessante nieuwe technologie met veelbelovende mogelijkheden. Een kleine computer, ingebed in een kunststofdrager ter grootte van een bankpas, biedt nieuwe mogelijkheden voor de burger/kaarthouder. Ook de combinatie van biometrische verificatiemethoden en de chipkaart lijkt een veelbelovende,



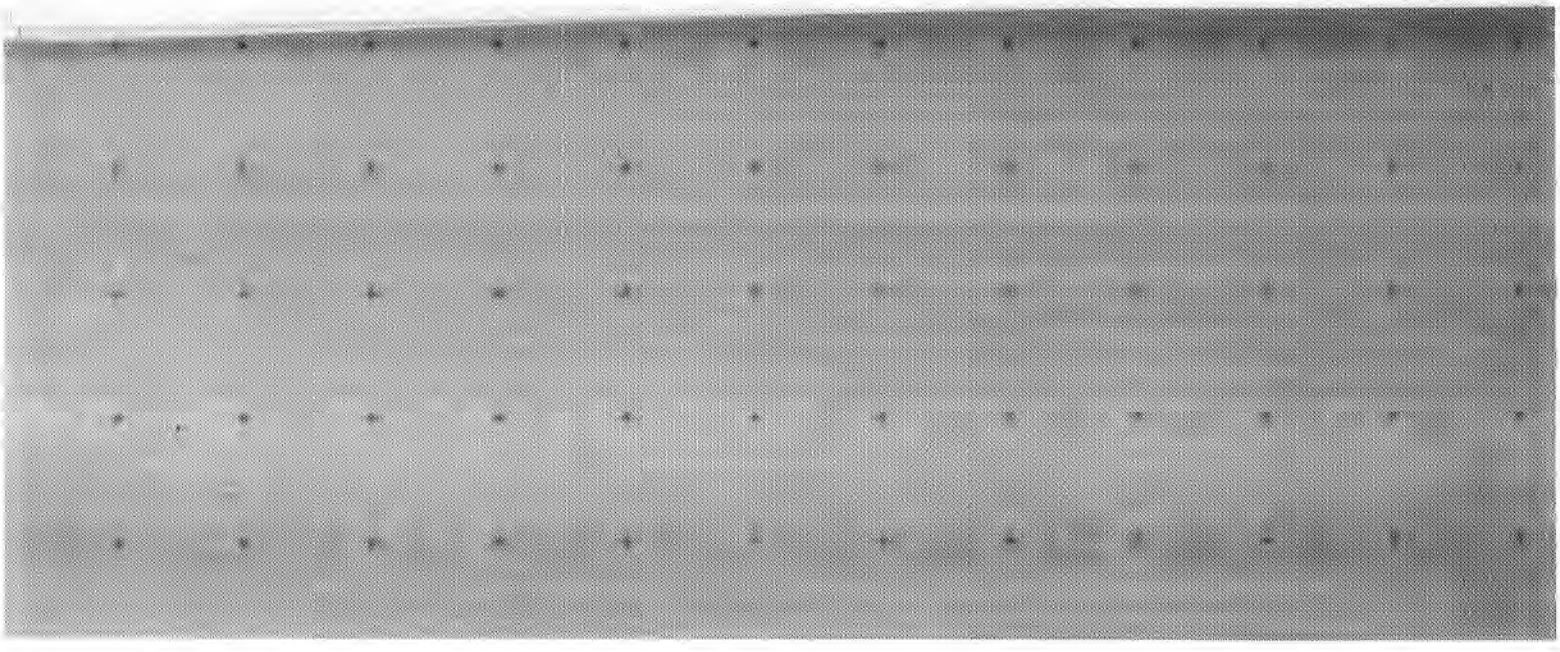
zowel uit een oogpunt van beveiliging als van dienstverlening.[1]

Zo biedt de geheugencapaciteit van de chip in de chipkaart de mogelijkheid in de identificatie en enrollmentfase het referentiepatroon of template van het biometrische kenmerk in de chipkaart zélf op te slaan. Dat biedt de mogelijkheid om de identiteit van de aanbieder ter plekke te verificeren, decentraal dus. Tot voor kort moest het opgeslagen 'biometrische profiel' van de kaarthouder uit een centraal computerbestand worden opgehaald. Daarvoor is een continue, dure en relatief veel tijd vergende 'on line' verbinding nodig tussen het kaartleesstation en het centrale bestand. Een ander nadeel vormt de noodzaak van een centrale database met biometrische gegevens van alle kaarthouders: een privacy-bedreigend risico.

Naast de geheugencapaciteit neemt ook de verwerkingskracht van de chipkaart nog steeds toe. Hierdoor wordt het mogelijk de vergelijking van het door de kaarthouder aangeboden biometrisch kenmerk met de in de kaart opgeslagen referentiewaarde door een aparte coprocessor in de kaart zelf te laten doen. Tot voor kort gebeurde dit altijd in het kaartleesstation of in het aan het leesstation gekoppelde computersysteem.

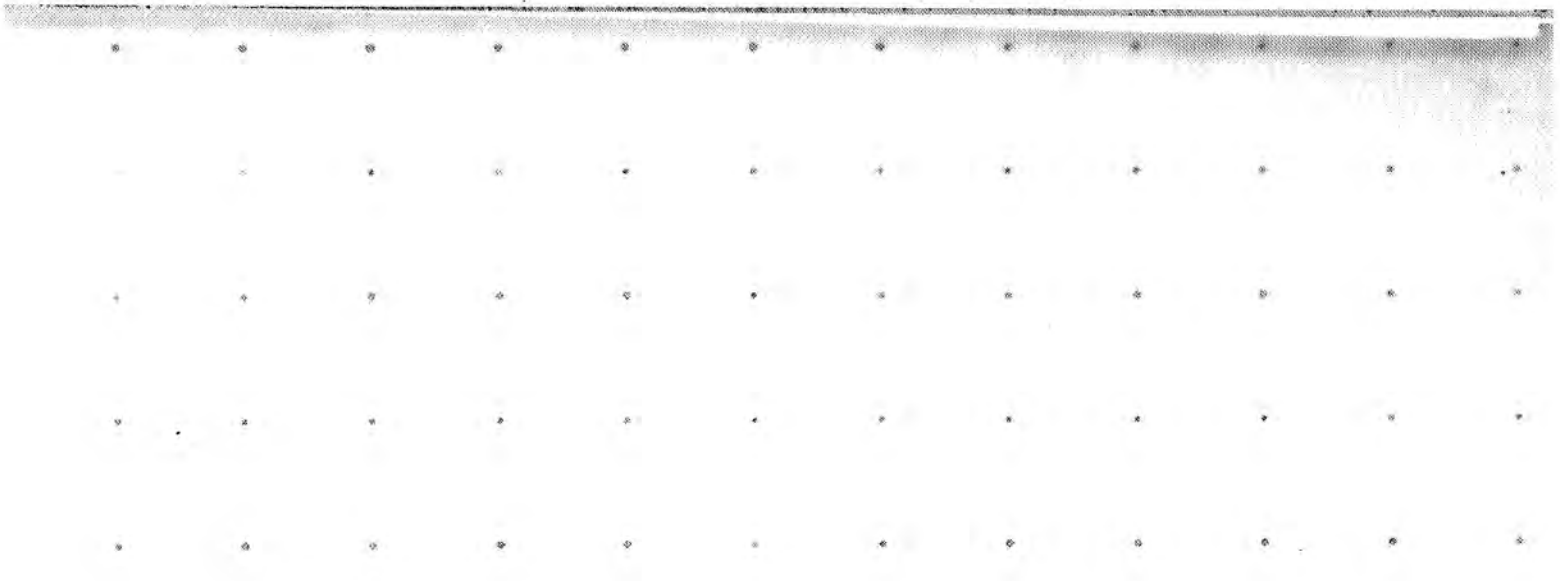
De volgende stap in de technische ontwikkeling is dat ook het leesstation voor een biometrisch kenmerk in de kaart zelf is geïntegreerd. Medio 1998 zijn de prototypen van een flinterdunne vingerafdruklezer, ingebed in een chipkaart, op de markt verschenen. Bij deze opzet komt de vingerafdruk dus noch tijdens de eerste vastlegging van de gegevens, noch tijdens de gebruiksfase buiten de kaart. De kaart geeft alleen een signaal af: de juiste persoon houdt de kaart vast, ja of nee.

[1] Biometrie en chipkaart, een unieke combinatie?, *zie literatuurlijst*



Biometrie: overwegingen

Overheid, burger en biometrie **Criminaliteitspreventie**



Wanneer de overheid biometrie wil toepassen, dient zij zich bewust te zijn van de voor- en nadelen. Voordelen zijn bevordering van de dienstverlening (de burger hoeft niet meer allerlei pincodes te onthouden) en toegenomen zekerheid dat producten en diensten alleen worden verstrekt aan de juiste persoon, met andere woorden aan degenen die daar recht op hebben. Biometrie kan zo helpen om fraude, misbruik en oneigenlijk gebruik van allerlei voorzieningen en regelingen tegen te gaan. Nadelen van biometrie zijn problemen met maatschappelijke acceptatie en de kosten van de systemen. Een aandachtspunt vormen ook de organisatorische consequenties.

Maatschappelijke acceptatie

Iets kan tot de technische mogelijkheden behoren en bijdragen aan de fraudebestrijding, maar daarmee nog niet maatschappelijk acceptabel zijn. Het Nationaal Chipkaart Platform (NCP) is sinds jaar en dag een warm voorstander van biometrie en één van de voornaamste pleitbezorgers. Deze organisatie heeft juist naar die maatschappelijke acceptatie van biometrie een onderzoek laten doen. Hiertoe zijn experts van banken en overheid om hun mening gevraagd. De algemene teneur van de reacties was, dat men in bepaalde situaties biometrie maatschappelijk toepasbaar achtte, maar bedenkingen had ten aanzien van de rijpheid van de techniek. Het aantal onterechte weigeringen en onterechte acceptaties zou bij de verschillende biometrische technieken nog te hoog liggen.

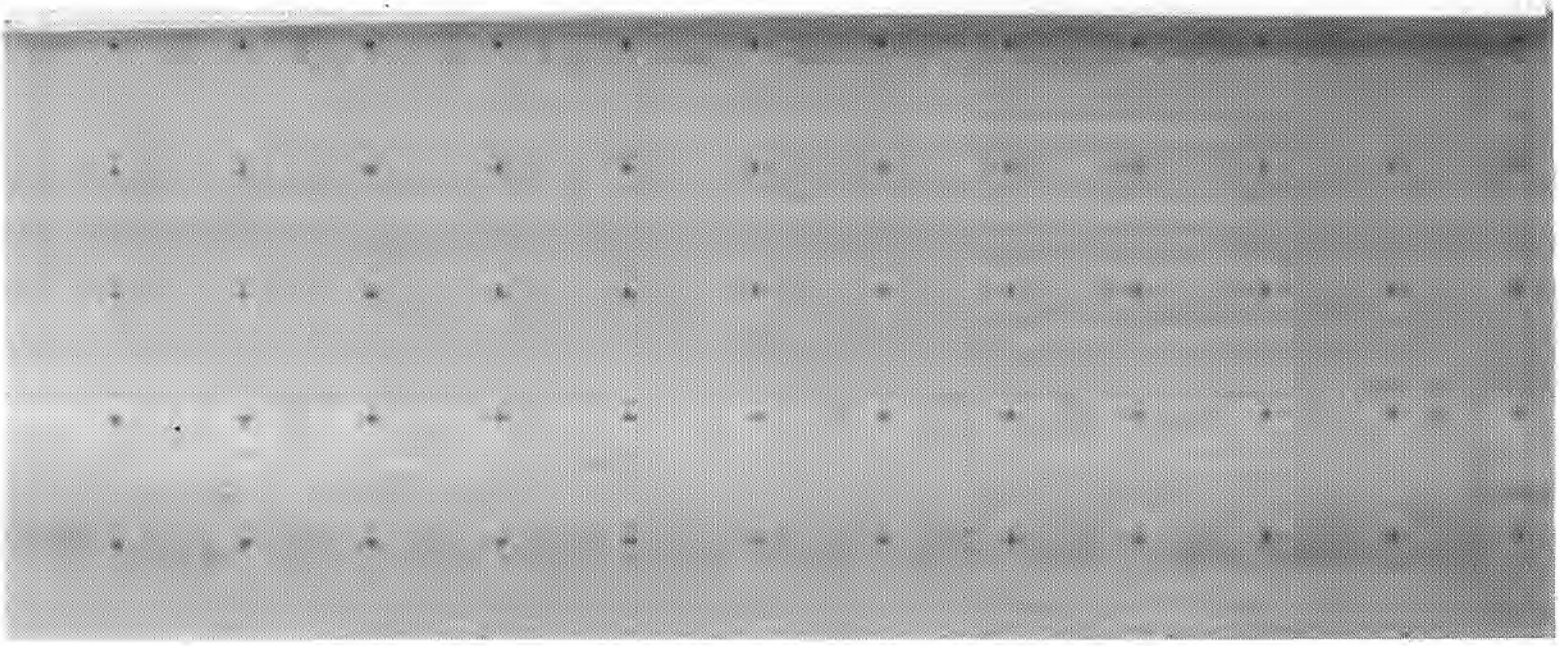
Om ook op praktisch niveau meer inzicht te krijgen in deze punten, heeft het NCP in zijn demonstratieopstelling van de Open Infrastructuur voor Chipkaarttoepassingen te Den Haag, twee van deze biometrische technieken nader onderzocht. Om een wat breder beeld te krijgen is daarbij gekozen voor één biometrisch handelingskenmerk (druk en snelheid van de handtekening) en één fysiek kenmerk (handgeometrie). De proef heeft 18 maanden gelopen en inzicht gegeven in de technische bruikbaarheid en in de reacties van het publiek dat de demonstratieopstelling bezoekt. De technische resultaten zijn redelijk positief en over de acceptatie valt bij het bezoekend publiek niet te klagen. Er zijn onder de ruim 4000 bezoekers van Chipkaart World geen personen geweest die geweigerd hebben hun biometrische karakteristieken te verstrekken.

Het Ministerie van Binnenlandse Zaken heeft deze input gebruikt bij het formuleren van zijn beleidsstandpunt rond het gebruik van biometrie bij reisdocumenten. Daarbij zijn tevens de resultaten betrokken van een mede door het NCP geïnitieerd onderzoek naar de juridische aspecten van biometrie.[1]

In juni 1998 heeft de Staatssecretaris van Binnenlandse Zaken zijn beleidsvoornemens besproken met de Tweede Kamer van de Staten Generaal. In het kort komen deze erop neer dat in 2001 de bestaande Rijksidentiteitskaart (met reismogelijkheden binnen Europa) als chipkaart zal worden uitgevoerd. Deze nieuwe generatie identiteitskaart zal worden voorbereid op de veelbelovende biometrietechnologie, maar daadwerkelijke invoering van biometrie zal pas daarna gebeuren.

De gezamenlijke gemeenten hebben specificaties ontwikkeld voor een Burger Service Kaart die de Gemeentelijke dienstverlening - via de extra mogelijkheden van de chiptechnologie - moet ondersteunen. Voor betrouwbare identiteitsvaststelling is daarbij al wél de inzet van biometrie voorzien. Verder zijn er initiatieven om biometrie in relatie met de chipkaart in de gezondheidszorg in te zetten. Chipkaart en biometrie zijn dus in aantocht.

[1] Het lichaam als sleutel, *zie literatuurlijst*



De vraag van de brede maatschappelijke acceptatie staat echter nog steeds open.

Bij dit laatste punt speelt mee, dat er in Nederland nog geen nationaal beleidskader voor biometrie is vastgesteld. Individuele overheidsorganisaties en partijen uit het bedrijfsleven passen biometrie toe wanneer zij dat wenselijk achten. Iedere organisatie is daarin vrij, binnen de vigerende bepalingen van de Wet Persoonregistraties (en binnenkort de Wet Bescherming Persoonsgegevens). Dat betekent dat als enige randvoorwaarde geldt, dat biometrie een redelijk middel moet zijn in relatie tot het beoogde doel. Voor de juridische aspecten en de grondwettelijke toelaatbaarheid van biometrie, zie literatuurlijst: 'Het lichaam als sleutel'.

Kosten

De kosten van biometrische systemen zijn nu nog relatief hoog. De prijs van eenvoudige sensoren ligt inmiddels al onder de *f*100,-. De kosten voor een compleet biometrisch systeem (sensoren, het vergelijkingsalgoritme, apparatuur en programmatuur voor het uitvoeren van de vergelijking etc.) variëren van enkele duizenden tot vele tienduizenden gulden.

Of er ook een sluitende 'business case' voor de inzet van biometrie is op te stellen, hangt dus volledig af van het doel dat de overheid daarmee wenst te bereiken.

Organisatorische aspecten

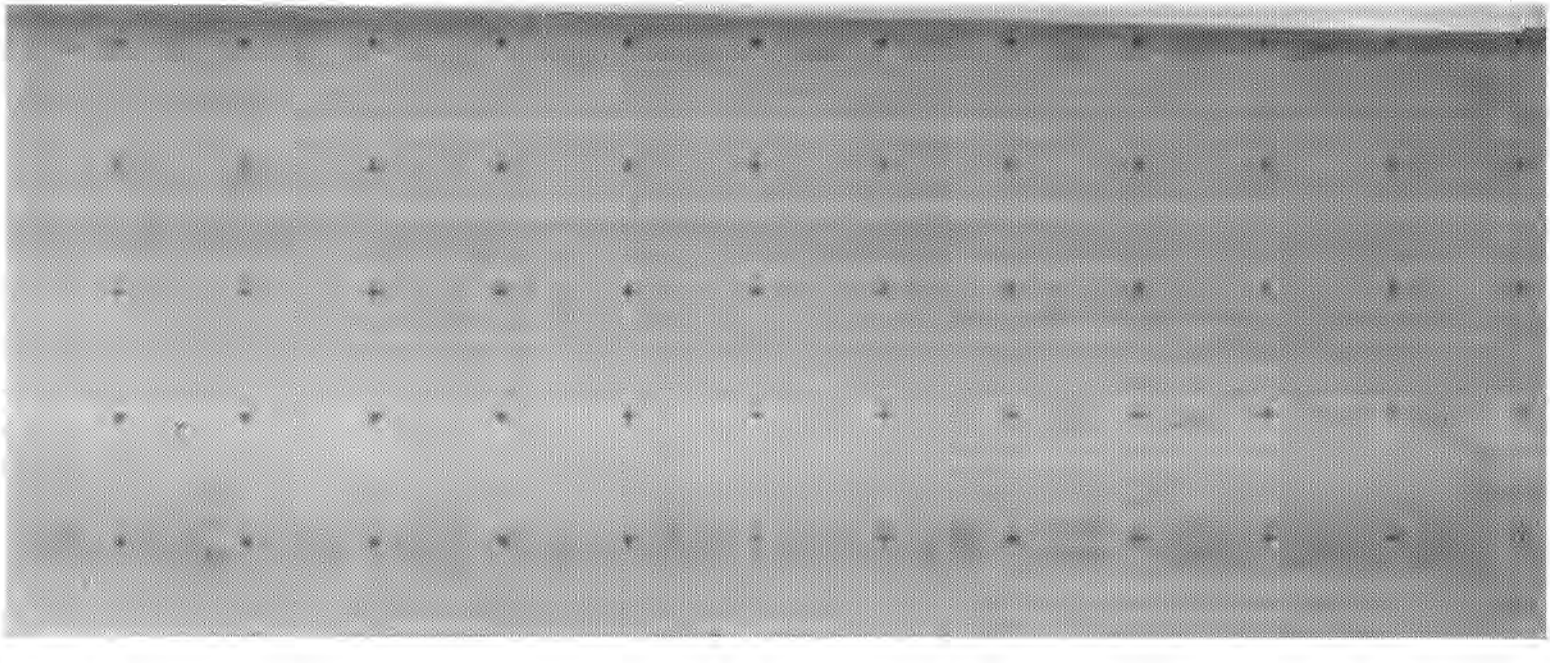
Invoering van biometrie in een systeem brengt organisatorische consequenties met zich mee. Zo is het proces van enrollment zeer arbeidsintensief en dus kostbaar. Ook behoeft de biometrische leesapparatuur het nodige onderhoud. Invoering van een biometrische techniek is dan ook alleen zinvol, wanneer dit in een duidelijke behoefte voorziet en logisch kan worden ingebed in het werkproces van de dienstaanbieder.

Is eenmaal een biometrisch identiteitsbewijs en verificatiemiddel met een voldoende graad van dekkendheid op de markt aanwezig (bijvoorbeeld de meergenoemde Burger Service Kaart), dan kan het al snel interessant worden voor een organisatie om zo'n kaart in zijn dienstverleningsprocessen toe te laten als verificatiemiddel voor de identiteit. Daarbij kan het gaan om overheidsorganisaties of de particuliere sector.

Welke biometrische techniek verdient de voorkeur?

Op deze vraag is geen algemeen antwoord te geven. Dit is namelijk sterk afhankelijk van de soort dienstverlening die een organisatie met biometrie wenst te ondersteunen. Een eerste vraag die men zich daarbij dient te stellen is, wat de karakteristieken van de toepassing zijn. Met andere woorden wat zijn de karakteristieken van de overheidsdiensten die men met biometrie wenst te gaan ondersteunen.

Zo maakt het een aanzienlijk verschil of men te doen heeft met burgers die veel of juist relatief weinig gebruik zullen maken van het systeem, of men te maken heeft met mensen die met het systeem willen meewerken of juist zullen proberen het systemen te frustreren etc. Ook is van belang of het een gesloten systeem is (voor een bepaalde wel omlijnde gebruikersgroep zoals bijvoorbeeld het eigen personeelsbestand), of een open systeem met een meer diffuse gebruikersgroep, zoals bijvoorbeeld alle inwoners van een Gemeente. Ook maakt het verschil of men apparatuur en programmatuur van meerdere leveranciers in het systeem wenst te accepteren of niet, etc.



Hierbij wordt onderscheid gemaakt in drie groepen van criteria:

A. De betrouwbaarheid van het systeem

Het is voor de overheid van belang dat men een zo betrouwbaar mogelijk biometrisch systeem in gebruik neemt. Naast de hiervoor genoemde criteria van maatschappelijke acceptatie en kosten speelt ook de mate van correct functioneren van het systeem een rol. Het is daarbij goed te bedenken dat geen enkel geautomatiseerd systeem voor 100% correct functioneert, dus ook een biometrisch systeem niet. Daarbij speelt mee dat een biometrische 'afdruk' of template nooit voor 100% gelijk is aan een eerdere afdruk. Dat geldt voor de vingerafdruk, het stempatroon en willekeurig welke andere techniek ook. Ook twee foto's die op verschillende tijdstippen van eenzelfde persoon zijn genomen lijken niet voor 100% op elkaar. Een daartoe opgeleid persoon die goed naar de foto's kijkt kan wel met een zekere mate van waarschijnlijkheid zeggen of deze foto's afbeeldingen van eenzelfde persoon zijn. De mate waarin eisen worden gesteld aan het 'verkeerd' beoordelen van personen is sterk afhankelijk van de toepassing. In het kader FAR (false acceptante rate) en FRR (false rejection rate) wordt dit nader uitgewerkt.

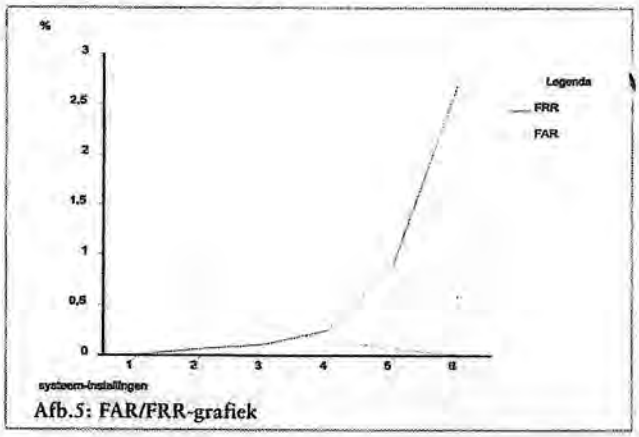
B. Het gebruiksgemak van het systeem

Een belangrijk keuzecriterium voor de overheid is het gebruiksgemak van het systeem. Omdat het veelal om toepassingen gaat die voor een breed publiek toegankelijk (moeten) zijn, zijn vriendelijke uitstraling en eenvoudige bediening noodzakelijk. Zo is de manier waarop iemand bijvoorbeeld 'geleid' wordt bij het afnemen van zijn biometrische karakteristieken van groot belang voor de gebruikersvriendelijkheid. Intussen zijn meetinstrumenten

FAR (false acceptanta rate) en FRR (false rejection rate)

Een biometrisch systeem kent intelligente rekenregels of 'algoritmen' om vast te stellen of twee templates voldoende op elkaar lijken om aan te mogen nemen dat deze van dezelfde persoon afkomstig zijn. De 'afwijkingen' waar het herkenningssysteem fouten maakt, worden aangeduid met FAR (false acceptante rate) en FRR (false rejection rate). Bij fouten van de eerste categorie gaat het om personen die door het systeem zijn geaccepteerd, terwijl dat eigenlijk niet had gemoeten. Bij de FRR gaat het om personen die eigenlijk door het systeem hadden moeten worden geaccepteerd, maar zijn geweigerd.

De FAR en FRR van biometrische systemen kunnen worden afgesteld, doch zijn aan elkaar gerelateerd. Als de FAR heel laag wordt ingesteld (bijvoorbeeld bij een toegangssysteem voor een wapenopslagplaats, waar men per se geen verkeerde personen binnen wil hebben) zal de FRR juist hoog zijn. Als men de FRR laag instelt, omdat men zijn klanten niet wil bruskeren (bijvoorbeeld in het pretpark Disneyland), zal de FAR relatief hoog worden en dus misschien wel eens iemand onterecht naar binnen kunnen slippen. De instelling van deze parameters hangt dus af van de wensen en eisen van de toepassingen waarbij men biometrie inzet. Het punt waar FAR en FRR gelijk zijn, noemt men EER (equal error rate). Een ideaal biometrisch systeem heeft een EER gelijk aan 0. Zo'n systeem bestaat niet. Men kan echter wel kiezen voor een systeem waarbij de waarde voor de EER laag ligt.



Afb.5: FAR/FRR-grafiek

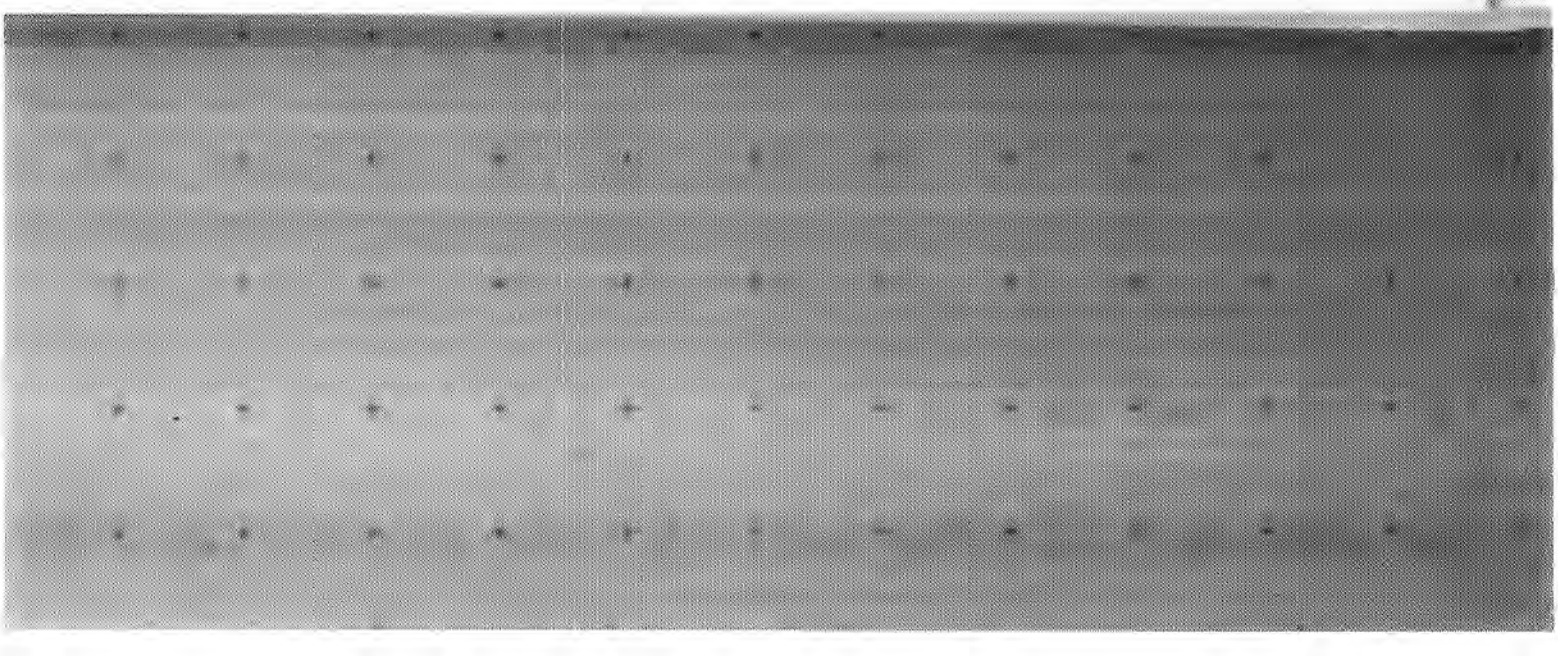
ontwikkeld om het gebruiksgemak van een systeem in kaart te brengen. Meer in het algemeen zijn de ergonomische aspecten bepalend hoe de gebruiker het systeem ervaart. Dit geldt ook voor bijzondere groepen, zoals gehandicapten.

C. De kwetsbaarheid van het systeem

Het systeem dient bestand te zijn tegen inbreuken, zowel van buitenaf als vanuit de eigen organisatie. Het mag bijvoorbeeld geen toegang verlenen bij nabootsing (bijvoorbeeld de stem), het systeem moet alleen levend weefsel accepteren, het moet bestand zijn tegen aanvallen op het mechanische, elektrische en programmatuurdeel van het systeem en het moet ook kunnen functioneren bij extremen in de omgevingsfactoren (temperatuurschommelingen, vocht, stof etc.). Ook moet het beveiligd zijn tegen verwijdering, ontkoppeling van kabels etc. zonder dat een dergelijke inbreuk sporen nalaat.

Onafhankelijke testinstituten

Het maken van een goed onderling vergelijk tussen de verschillende IT-leveranciers op de biometriemarkt en hun producten, is geen eenvoudige zaak. Een overheidsorganisatie kan uiteraard een eerste selectie maken aan de hand van leveranciersdocumentatie en gesprekken met vertegenwoordigers van de leveranciers. Vervolgens verdient het echter aanbeveling om - zeker bij een grootschalig project - advies van een onafhankelijke adviseur in te winnen. Dat kan bij IT-consultants, maar ook bij testinstituten. In Nederland zijn TNO en KEMA op dit gebied actief. In Europa is met behulp van de Europese Commissie het Europees testinstituut Biotest in het leven geroepen. Het NCP is bij deze ontwikkeling betrokken. In Engeland en Spanje zijn inmiddels testvoorzieningen gerealiseerd en kunnen verschillende systeemtypen onderling worden vergeleken. In Amerika is de San José University benoemd als nationaal biometrie-testinstituut.



Toekomst

Toekomst

De toekomst voorspellen is altijd een hachelijke zaak, met biometrie is dat niet anders. Na een langzame start in de afgelopen jaren staat biometrie echter aan de vooravond van een massale doorbraak. Apparatuur en programmatuur hebben zich de afgelopen jaren sterk ontwikkeld en zijn meer volwassen geworden. Standaard interfaces in de vorm van biometrie application interfaces (BAPI) zijn in opkomst. Lange tijd is biometrie het werkterrein geweest van kleine bedrijfjes die spannende nieuwe zaken wisten te ontwikkelen. Tegenwoordig komen ook de grotere spelers op de markt, zoals Microsoft (standaardvoorzieningen in Windows), Siemens (warmtepatroonherkenningssystemen en vingerafdruklezers) en SGS/ Thomson (vingerafdruklezers). Een bedrijf als NCR heeft inmiddels ook de nodige apparatuur (gezichtsherkenning) ontwikkeld. Dat mag als een teken van volwassenheid worden aangemerkt.

In Nederland is de biometrie in gebruik bij projecten als de Asielzoekerkaart, voor de toegangsbewaking in bepaalde gevangenissen, bij een project voor het snel in- en uitchecken van chauffeurs bij containervervoer in de Rotterdamse haven etc. Ook zijn er de nodige buitenlandse banken die met biometrie experimenteren.
Zij concentreren zich op geldautomaten. In de amusementsindustrie heeft het Amerikaanse Disneyland inmiddels de handgeometrie bij de toegangscontrole van de jaarabonnementhouders in zijn parken ingevoerd. Een sociale zekerheidskaart in Spanje met vingerafdruk is reeds in een oplage van 5 miljoen in gebruik. Al met al lijkt het erop, dat biometrie inmiddels zover uitontwikkeld is dat massale toepassing wereldwijd binnen bereik is.

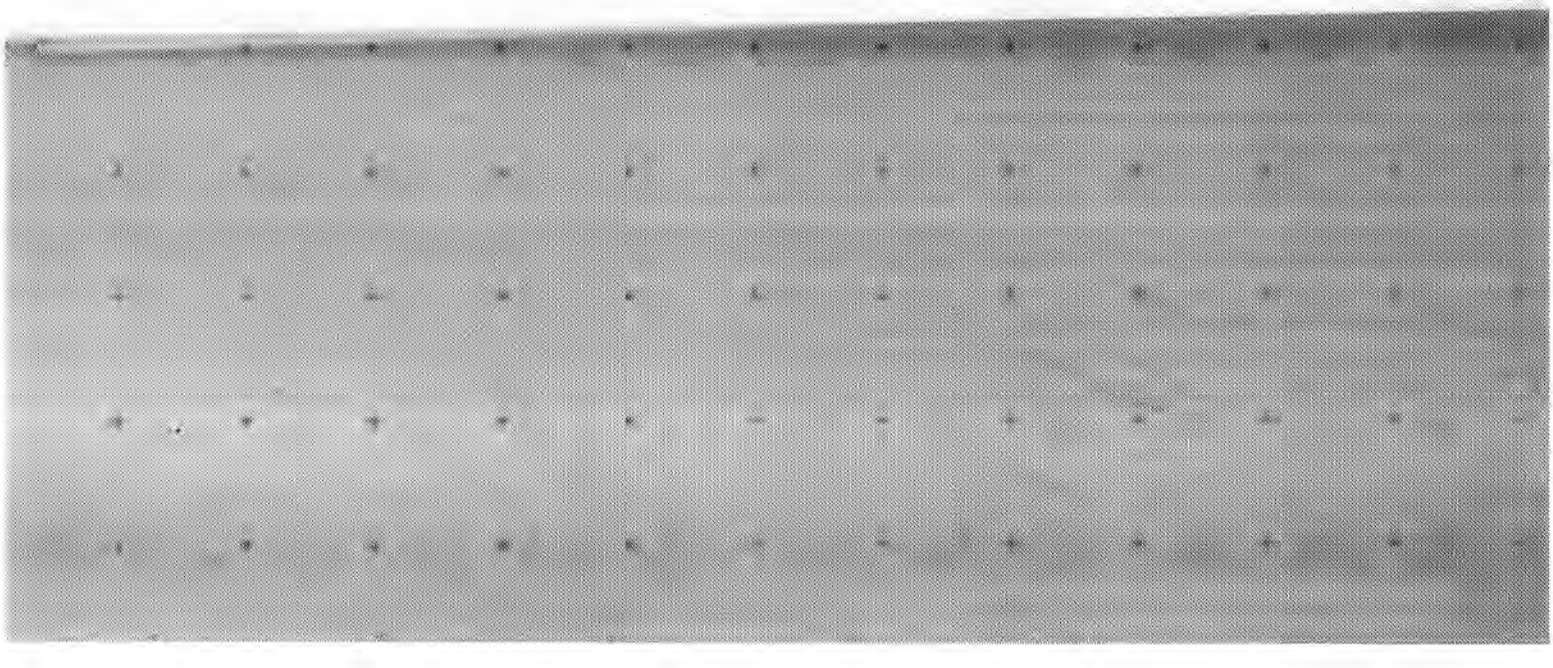
Praktijkcase Burger Service Kaart Haarlem

De Gemeente Haarlem is de eerste Gemeente die met de combinatie van chipkaart en biometrie ervaring wil opdoen. In een Haarlemse wijk is veel overlast ondervonden door fietsendiefstal. Op voorspraak van het wijkberaad, worden in de wijk vijf fietsenkluizen geplaatst. Iedere kluis heeft ruimte voor zo'n twintig fietsen.
De toegang tot deze fietsenkluizen wordt beveiligd met biometrie. Verder heeft het wijkberaad van de betreffende wijk voorgesteld de toegang tot een aantal achteringangen van woningen (gelegen aan een soort brandgang die achter de woningen loopt) via de Burger Service Kaart met biometrie te beveiligen.

De bewoners ervaren dit als een duidelijke verbetering van hun woonomgeving en een vermoedelijke bijdrage aan het terugdringen van de criminaliteit in hun woonomgeving. Wijkbewoners die dat wensen ontvangen van de Gemeente een chipkaart, die van de nodige administratieve persoonsgegevens is voorzien. De wijkbewoner dient de kaart persoonlijk bij het gemeentehuis op te halen. Alvorens hij of zij de kaart meekrijgt, wordt de handgeometrie van de betreffende persoon gemeten en op de kaart opgeslagen. Deze kaart is dus een ideaal-typische en - wat betreft de identificatie en verificatiefunctie - zeer complete Burger Service Kaart.

Uiteraard is het de bedoeling in dit experiment aanvullende maatregelen uit te proberen om allerlei praktische problemen aan te pakken. Een voorbeeld daarvan is de vraag of voor familie of vrienden het mogelijk gemaakt moet worden achterom te gaan of om iemands fiets uit de kluis te halen.

Tot zover lijkt het niet meer dan een basaal fysiek toegangscontrolesysteem. Maar er is meer. De administratieve gegevens op de kaart zijn ontleend aan de Gemeentelijke bevolkingsadministratie. Indien één of meer van



deze gegevens wijzigen (bijvoorbeeld het woonadres als gevolg van een verhuizing) en het recht op toegang tot de fietskluis resp. de achteringang voor de betreffende persoon niet meer van toepassing is, dan zal het systeem de toegang voor de betreffende kaarthouder blokkeren.

Ook heeft de Gemeente Haarlem het voornemen meerdere diensten via de kaart toegankelijk te maken. Daarbij moet gedacht worden aan het ontsluiten van (gemeentelijke) diensten via Internet. Ook op dit punt kan met behulp van de chipkaart een gedifferentieerd toegangs- en autorisatiebeleid worden gevoerd. Differentiatie is desgewenst mogelijk tot op het niveau van de individuele kaarthouder.

Gewin en gemak

Wat wereldwijd en dus ook in Nederland ontbreekt, is een visie van de zijde van de overheid op het gebruik van biometrie. Tot op heden wenst de overheid kennelijk geen maatschappelijke of technische randvoorwaarden te stellen aan het gebruik van biometrie.

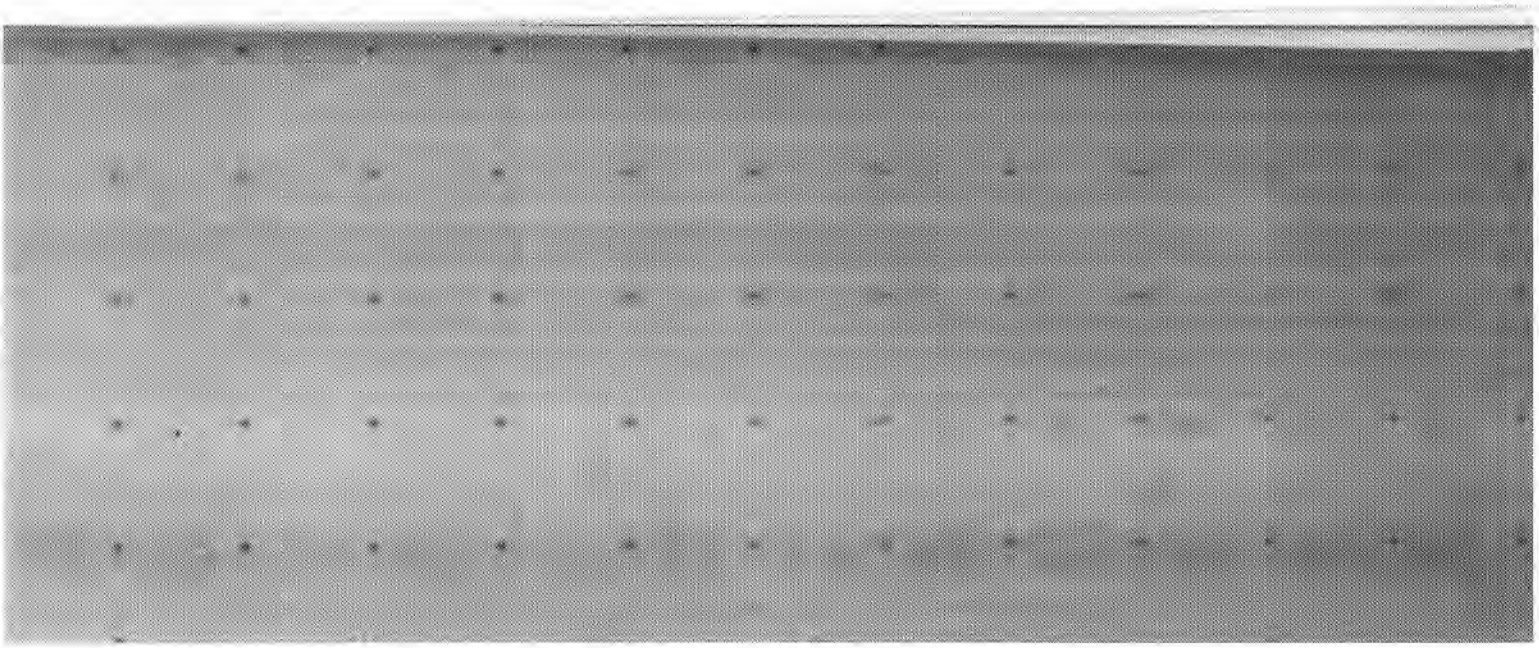
De overheid kiest derhalve dus niet voor een randvoorwaarden- of regelscenario, maar voor een scenario van marktwerking. Daarbij geldt uiteraard de rechtsbescherming zoals die in de Wet Persoonsregistraties en zijn opvolger, de Wet Bescherming Persoonsgegevens, is opgenomen.

Binnen dit marktwerking scenario kan de overheid als grote aanbiedende partij natuurlijk wel een dominante rol gaan spelen. De Burger Service Kaart en de Elektronische Identiteits Kaart van het Ministerie van BZK hebben zeker de nodige potentie op dat terrein.

In dit scenario zullen er echter meerdere biometrische technieken naast elkaar worden ingevoerd. Internationaal is er nog geen overeenstemming, welke technologie uiteindelijk 'winning' zal blijken te zijn. Het is niet te gewaagd om te veronderstellen dat bij ongewijzigd beleid in de verschillende landen binnen en buiten Europa verschillende technieken naast elkaar zullen worden gehanteerd. Net als de veelheid aan pincodes, komt er dan een veelheid aan biometrische technieken. Een lijn die zich wellicht zal doorzetten bij de Nederlandse Gemeenten, al dan niet in combinatie met de Burger Service Kaart.

De 'redding' komt wellicht uit de financiële sector. De komst van de Euro is daarbij uiterst strategisch. Eén Europese munt zal naast economische voordelen en voordelen van consumentengemak ook tot nieuwe activiteiten van het vervalsersgilde leiden. Bestrijding van dit soort muntfraude is alleen op Europees niveau mogelijk. Daarbij kan ook aan biometrie worden gedacht. Voor een uniforme Europese biometrietoepassing zal standaardisatie op één technologie noodzakelijk zijn, wil het geheel financieel tot de mogelijkheden behoren.

Hoe het ook zij, één biometrische techniek of meerdere, het grote voordeel en de winst voor de consument zijn daar. Anders dan met de verschillende pincodes die niet meer te onthouden zijn, heeft de burger zijn gezicht, vingerafdruk, handgeometrie, dynamische handtekening en wat al niet meer altijd bij zich. Zaken die snel op hun 'echtheid' en 'bij de persoon horen' te controleren zijn. Eindelijk dus een burgervriendelijke oplossing voor het identificatie- en verificatievraagstuk. Of met de woorden van de inleiding, een bruikbare oplossing die werkelijk Gewin (van tijd) en Gemak (altijd bij je) voor de burger kan bieden.



Achtergrondinformatie

T&S Criminaliteitspreventie Programma Technologie & Samenleving

De samenleving wordt geconfronteerd met een groot aantal maatschappelijke vraagstukken, zoals congestie, criminaliteit, het gevoel van onveiligheid en het gebrek aan zorg aan huis. De overheid is van mening dat technologie op deze terreinen meer kan bijdragen aan oplossingen dan tot dusver is gebeurd. Het programma Technologie & Samenleving (T&S) heeft dan ook tot doel projecten te stimuleren die leiden tot een betere benutting van technologische mogelijkheden bij het aanpakken van maatschappelijke problemen. De T&S-benadering is daarmee vooral market-pull van aard en niet technology-push.

Momenteel kent het programma zes deelprogramma's:

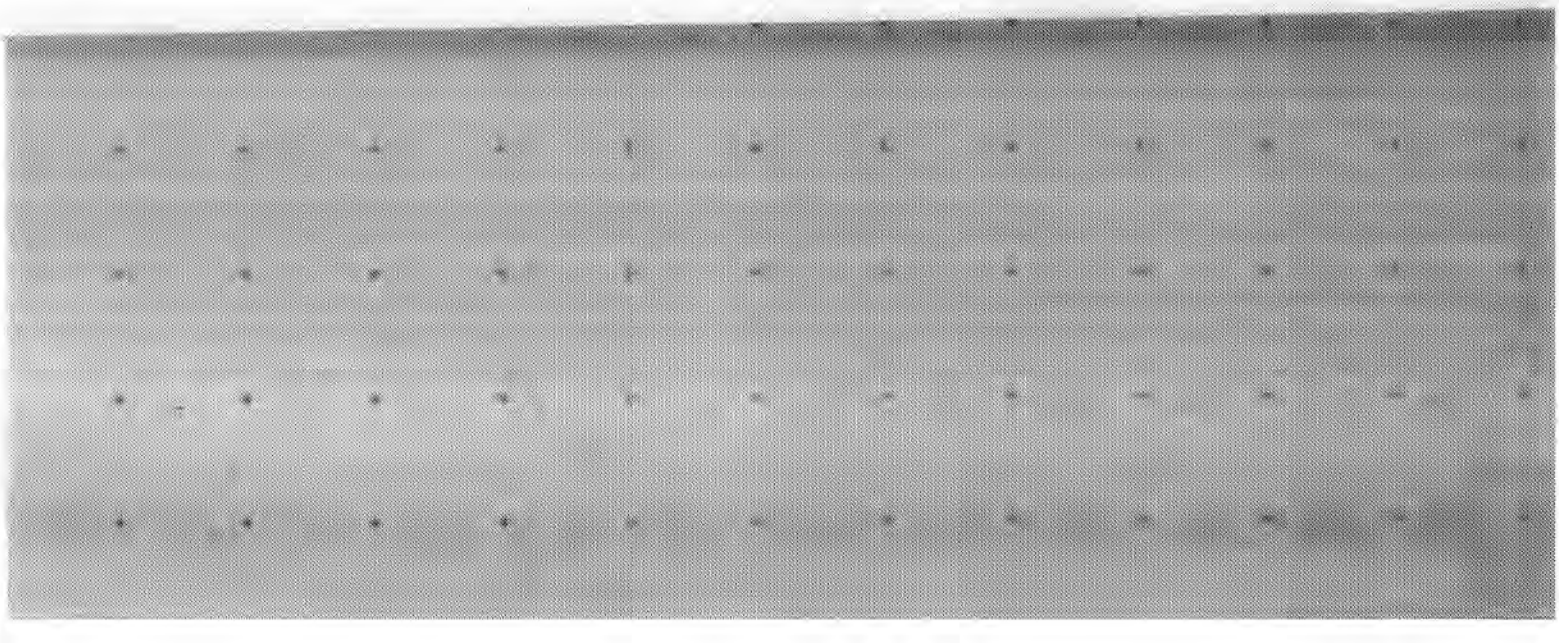
- Ouderentechnologie
  (indienen van aanvragen is niet meer mogelijk)
- Criminaliteitspreventie
- Transmurale Zorg
- Leren in de werkomgeving
- Gehandicapten
  (indienen van aanvragen is niet meer mogelijk)
- (Re)integratie in arbeid

Opzet programma

T&S is in 1995 gestart met de deelprogramma's Ouderentechnologie en Criminaliteitspreventie. Elk deelprogramma heeft een looptijd van drie jaar en elk jaar worden enkele nieuwe deelprogramma's gepakt.
In 1996 is een algemene verkenning uitgevoerd naar onderwerpen die zich lenen voor een uitwerking in een T&S-deelprogramma. Hieruit is een lijst gegenereerd met relevante maatschappelijke probleemgebieden, die met een betere benutting van technologische mogelijkheden aangepakt kunnen worden. Zo zijn op basis van de verkenning eind 1996 de deelprogramma's Transmurale zorg en Leren in de werkomgeving gekozen.
Ook kunnen bijvoorbeeld vanuit departementen programma's worden geïnitieerd naar aanleiding van een actuele, geconstateerde behoefte.

Criminaliteit is een belangrijk item in zowel het welzijnsgevoel voor de burger als gegeven de maatschappelijke kosten.

Ieder deelprogramma start met een technologiescan: een verkennende studie die inzicht geeft in de (technologische) stand van zaken en die informatie oplevert over de terreinen, waarop het deelprogramma kan bijdragen aan de ontwikkeling van kansrijke producten en diensten.



Het resultaat van deze scan is het benoemen van een aantal aandachtsgebieden en het zo mogelijk aangeven van kansrijke projecten.

De actielijnen binnen het deelprogramma Criminaliteitspreventie zijn: Sociaal Veilig Ontwerpen, Identificatie, Beveiligingssystemen, Communicatie met de politie en Persoonlijke Veiligheid.

Partijen uit het veld (professionals, bedrijven, kennisinstituten) worden uitgenodigd met projectvoorstellen te komen. De projecten dienen met de inzet van technologie een herkenbare oplossing te bieden voor een maatschappelijk probleem en moeten de consument dus laten zien dat met technologie resultaten kunnen worden bereikt 'waar de samenleving iets aan heeft'. De te ontwikkelen producten en diensten moeten binnen drie jaar op de markt zijn gebracht. Vaak zal het daarom gaan om bestaande technologie of technologie die op korte termijn beschikbaar komt.

Voorbeelden van projecten binnen het thema Criminaliteitspreventie zijn: elektronische aangifte, biometrische identificatie een projectendatabase met best practices, elektronisch huisarrest, camerabewaking in de openbare ruimte, sociaal veilige verlichting etc.

Kennisverspreiding

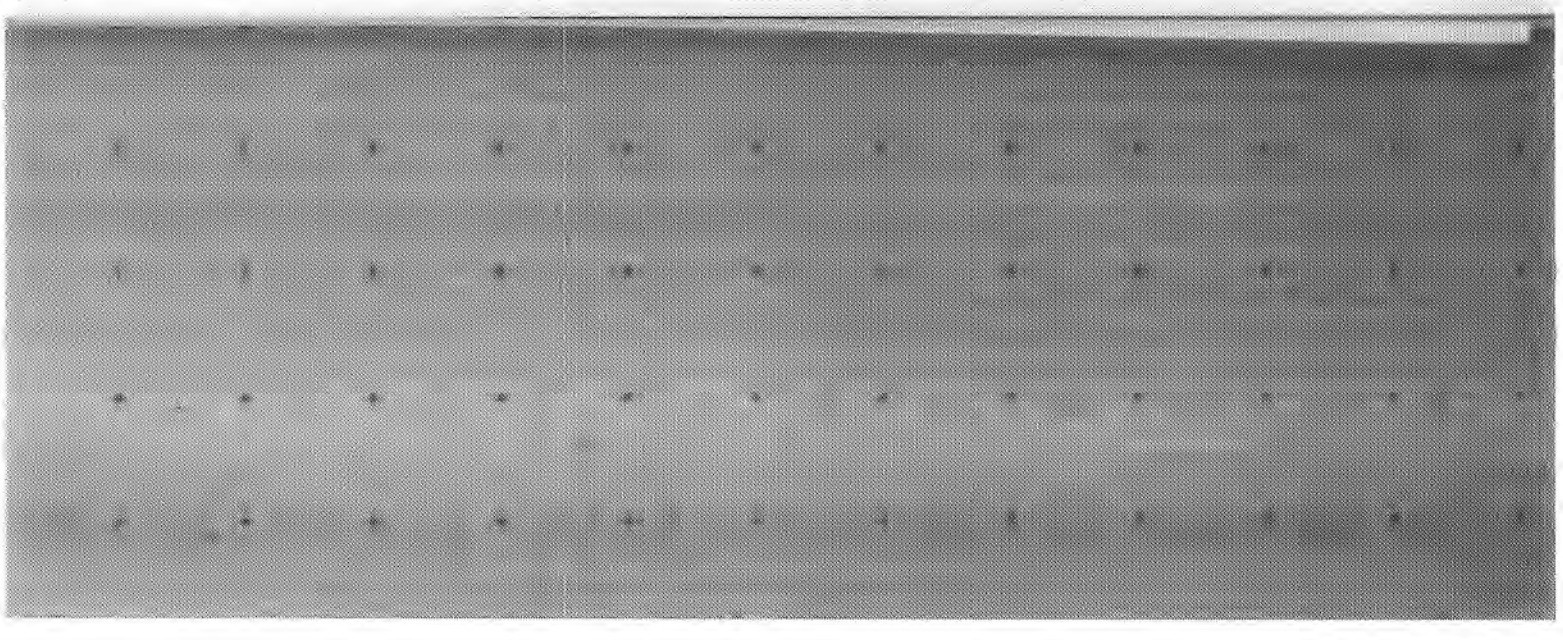
Een belangrijk onderdeel van het T&S-programma is de verspreiding en overdracht van de opgedane kennis en ervaringen in het programma. Via publiciteit en verschillende activiteiten, zoals workshops wordt aandacht gevraagd voor de betreffende problematiek.

Een voorbeeld daarvan is de T&S publicatiereeks, waarin resultaten van projecten en studies verschijnen. Ervaringen die bij de voorbeeldprojecten zijn opgedaan worden vastgelegd en overgedragen aan de diverse doelgroepen.
De resultaten uit de projecten laten zien dat bedrijven en andere organisaties in het programma met technologische én marktgerichte oplossingen een bijdrage leveren aan maatschappelijke problemen.

Organisatie

Elk deelprogramma wordt begeleid door een projectgroep, die bestaat uit vertegenwoordigers van de betrokken departementen en mogelijk andere (koepel)organisaties. De projectgroep is verantwoordelijk voor de inhoudelijke invulling van het programma en beoordeelt de projectvoorstellen. Een Stuurgroep is verantwoordelijk voor de aansturing van het totale programma.

Thema	Partijen vertegenwoordigd in de Projectgroepen
Ouderentechnologie	VWS, VROM, EZ
Criminaliteitspreventie	BZK, Justitie, EZ
Transmurale Zorg	VWS, EZ, Rathenau Instituut, TNO Preventie en Gezondheid, ZON (ZorgOnderzoek-Nederland), Stichting Ziekenhuis Verplaatste Zorg
Leren in de werkomgeving	OCW, SZW, EZ, FNV, VNO-NCW, MKB Nederland
Gehandicapten	VWS, EZ, Open Ankh instellingen
(Re)integratie in arbeid	SZW, VWS, EZ, CNV, MKB-Nederland, BOA, LISV, CSO, NCCZ



Senter, uw partner bij het ondernemen

Om het Nederlandse bedrijfsleven het hoofd te laten bieden aan de internationale concurrentie op de wereldmarkt, wil de Nederlandse overheid bedrijven stimuleren om meer aan onderzoek, ontwikkeling en de toepassing van kennis te doen. Samenwerking met andere bedrijven en met kennisinstellingen staat hierbij hoog in het vaandel. De overheid wil dat bedrijven en kennisinstellingen samen op een hoger kwaliteitsniveau gaan opereren en dat de Nederlandse kennisinfrastructuur wordt versterkt.

De overheid wil het kennisniveau van het Nederlandse bedrijfsleven bevorderen door:

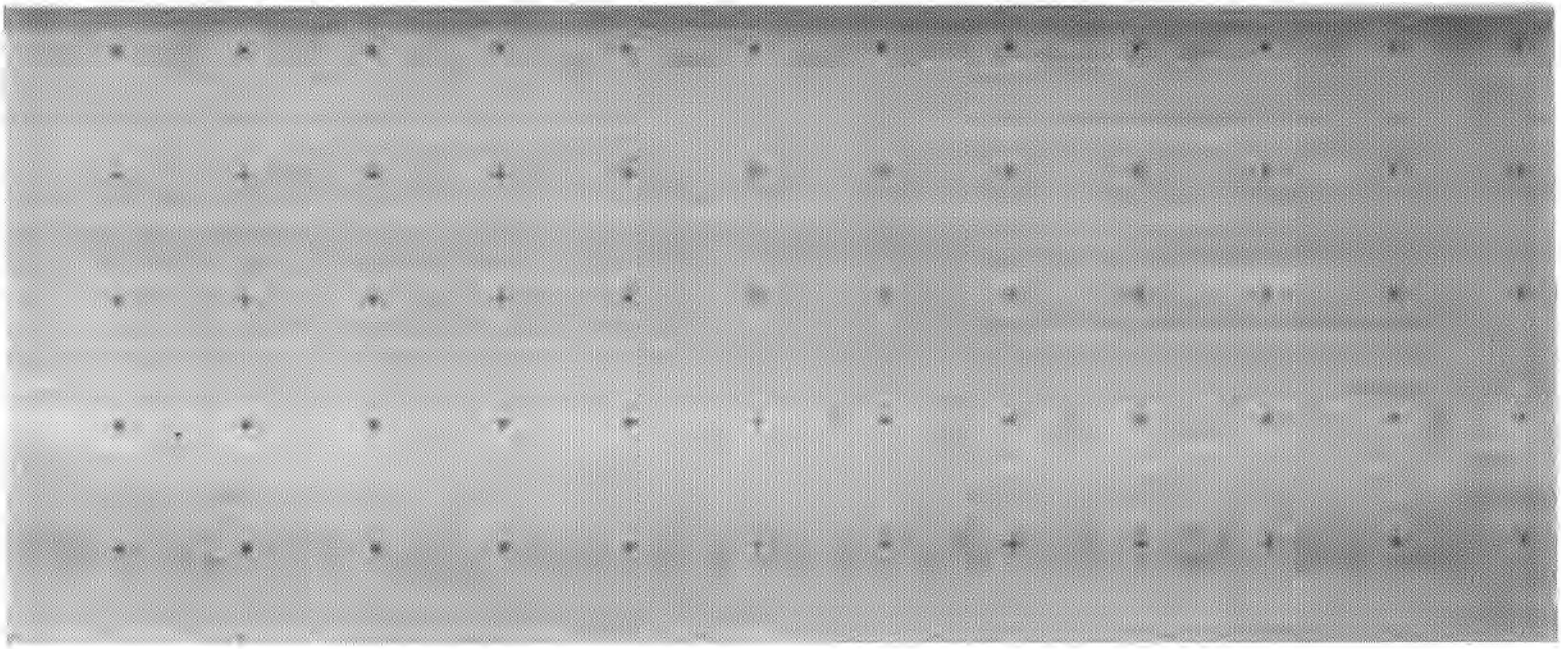
- innovatie te vergemakkelijken;
- meer uit investeringen in kennis te halen door een betere uitwisseling tussen de vraag naar en het aanbod van kennis;
- meer in te spelen op de kansen die nieuwe technologieën bieden (want meer kennis betekent in de praktijk vooral meer technologie).

Senter is een agentschap van het Ministerie van Economische Zaken dat gespecialiseerd is in het uitvoeren van stimuleringsmaatregelen voor de overheid op het gebied van technologie, energie, milieu, internationale samenwerking en export. Daarnaast is ook het adviseren van bedrijven over stimuleringsprojecten een kernactiviteit van Senter. In de derde plaats houdt de organisatie zich bezig met het Nederlandse kennisnetwerk, tussen bedrijven onderling en tussen bedrijven en kennisinstellingen. Ten slotte biedt Senter hulp wanneer u internationaal samen wilt werken of als u wilt exporteren.

In opdracht van het Ministerie van Economische Zaken voert Senter het programmamanagement uit voor het programma Technologie & Samenleving. Voor ieder thema is een secretaris aangewezen. Deze kan u informeren over het programma en de lopende activiteiten en u kunt bij hem of haar terecht voor het bespreken van een projectidee en het indienen van een projectvoorstel.

Wilt u meer informatie over de subsidie- en kredietmogelijkheden van Senter dan kunt u contact opnemen met het KMO-InformatieSenter. Dit dagelijks geopende telefonische informatiepunt is speciaal, maar niet uitsluitend voor kleine en middelgrote ondernemingen onder telefoonnummer (070) 361 02 77.

Senter Den Haag
Postbus 30732 2500 GS Den Haag
Telefoon (070) 361 0597/339
Telefax (070) 361 4430
Internet www.senter.nl



Nationaal Chipcard Platform

Stichting Nationaal Chipcard Platform is opgericht in 1994, met als doel het bijdragen aan een verantwoorde invoering van chipkaarttechnologie in Nederland. Naast diverse voorlichtende en ondersteunende publicaties hebben de deelnemers (zo'n 50 partijen uit de sectoren Overheid, Financiën, Vervoer, Zorg en IT) een afsprakenstelsel ontwikkeld voor een OIC; een Open Infrastructuur voor Chipkaarttoepassingen. Voornaamste kenmerken van deze OIC zijn multifunctionaliteit en interoperabiliteit. Dit houdt in dat chipkaarten met daarop diverse toepassingen in chipkaartlezers van verschillende systeemaanbieders te gebruiken moeten zijn. Het afsprakenstelsel is erkend door het Nederlands Normalisatie Instituut en heeft de officiële status gekregen van Nederlandse Praktijk Richtlijn (NPR7402).

Stichting Nationaal Chipcard Platform
Postbus 262
2260 AG Leidschendam
Telefoon 070-3010817
Telefax 070-3206614
Website http://www.dds.nl/~ncp

Acquest

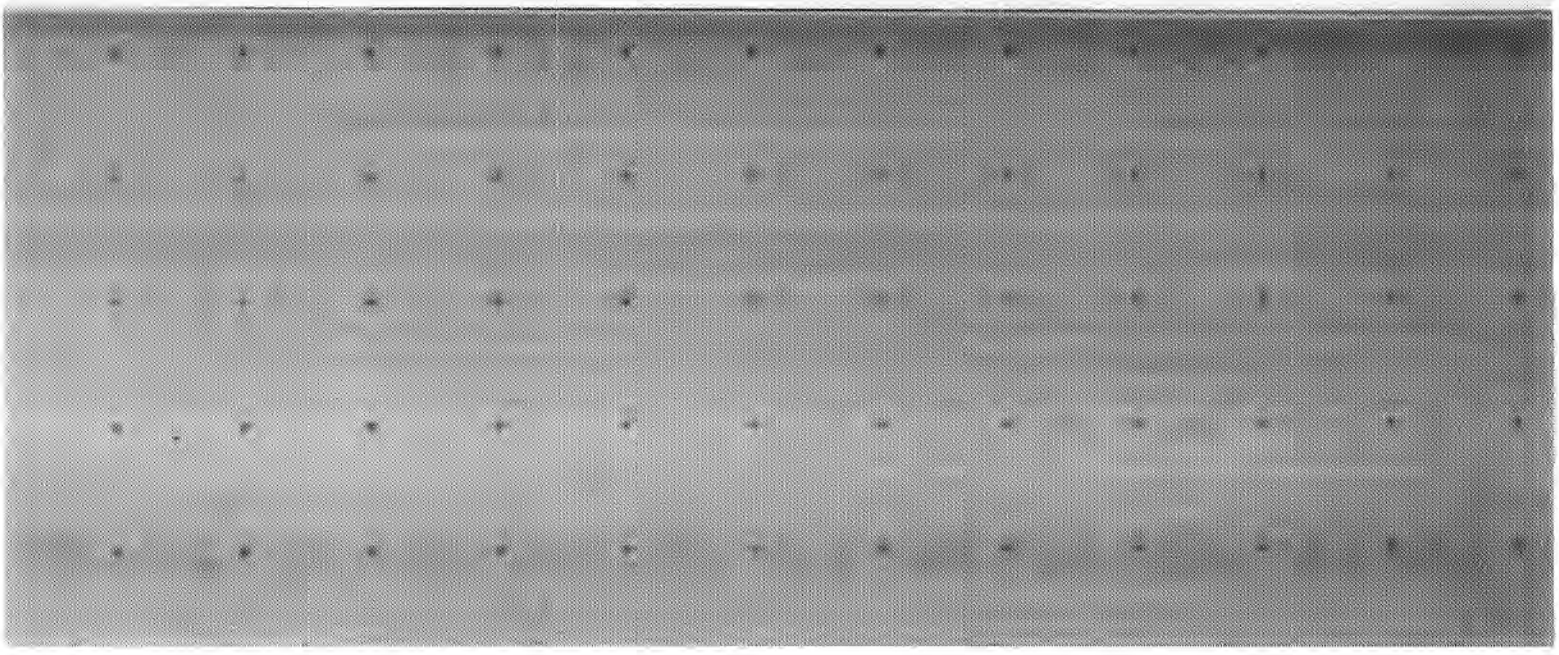
Organisatie Adviesbureau Acquest combineert kennis en vaardigheden op het gebied van inhoud, (bedrijfs)processen en informatie- en communicatietechnologie. Acquest is actief binnen diverse sectoren: zorg en welzijn, gemeentebeleid, maatschappelijke ontwikkelingen.

Acquest stelt haar deskundigheid ter beschikking om te bevorderen dat ICT nut heeft voor burgers, ongeacht hoe zij zich noemen: ouderen, jongeren, gehandicapt, nieuwkomer; en ongeacht hun herkomst, situatie en achtergronden. Daarbij gaat het om specifieke applicaties, inter/intranet-achtige voorzieningen en chipkaart ontwikkelingen.

Acquest is in staat projecten te helpen formuleren, daar steun voor te zoeken en het projectmanagement op zich te nemen. Tevens voert Acquest verwante activiteiten uit zoals trainingen, ontwikkeltrajecten en onderzoek (evaluatie, haalbaarheid ed.).

Acquest is op het ogenblik onder andere betrokken bij Overheidsloket 2000, Sein 2001, de Burger Service Kaart ontwikkeling, ICT projecten in de zorg, evaluaties, adviezen en projectmanagement voor DG XIII van de Europese Commissie.

Acquest Consultancy BV
Hoofdstraat 2, 2351 AJ Leiderdorp
Telefoon 071-5419594



Literatuurlijst

1 In de kaart gekeken, De chipcard strategisch bezien
SMO / NCP publicatie,
J. van Arkel e.a. 1995

2 Fundamentele technische keuzen voor een Open Infrastructuur voor chipkaartoepassingen (OIC) en biometrische verificatiemethoden voor zo'n infrastructuur
Afstudeerscriptie Ron Kivits,
in opdracht van het Nationaal Chipkaart Platform,
mei 1995

3 Biometrie en de chipkaart, een unieke combinatie?
Afstudeerscriptie Alexandra van der Tuin
in opdracht van het Nationaal Chipkaart Platform,
augustus 1996

4 Het lichaam als sleutel,
Juridische beschouwingen over biometrie
Robert van Kralingen, Corien Prins, Jan Grijpink,
Jan van Arkel,
IteR-reeks,
mede in opdracht van het Nationaal Chipkaart Platform,
1997

5 The Biometric Report, A research report on systems, equipment, costs, advantages and markets
SJB Services, 1998

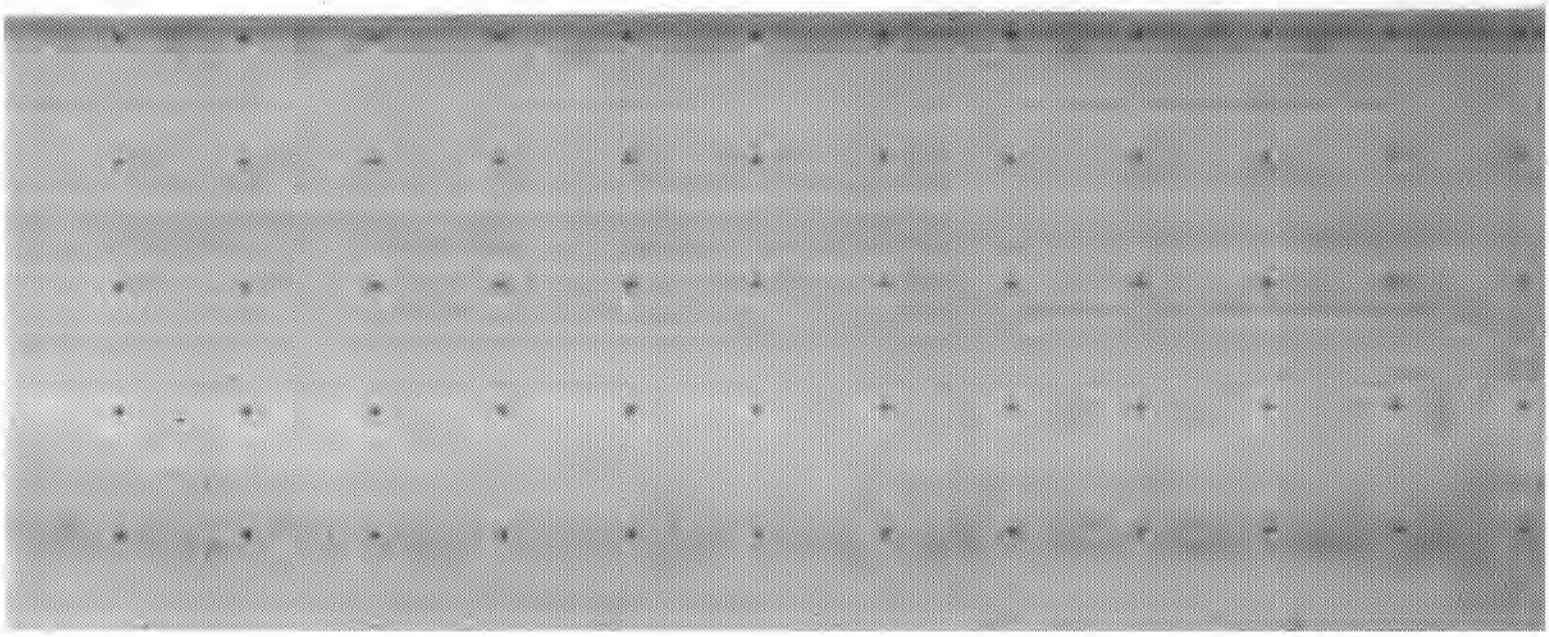
6 BIOTEST, Project on BIOmetric TESTing Services, co-funded by the European Commission, ESPRIT 21978-1998
Het Nationaal Chipkaart Platform is bij dit project betrokken als evaluator.
Materiaal is deels vertrouwelijk.

7 Smart Cards '98, London
Conference Proceedings

8 Card Tech/Secur Tech 1998, Washington
Conference Proceedings

9 Cards Asia '98, Singapore
Conference Proceedings

10 Functionele Specificaties Burger Service Kaart
Werkgroep Burger Service Kaart II, april 1998



Ouderentechnologie

Criminaliteitspreventie

Transmurale zorg

Leren in de werkomgeving

Deze publicatie maakt deel uit van de serie Technologie & Samenleving. In deze serie staan vier thema's centraal: ouderentechnologie, criminaliteitspreventie, transmurale zorg en leren in de werkomgeving. Technologie loopt als een rode draad door deze thema's heen en biedt een oplossing voor een maatschappelijke ontwikkeling. Criminaliteit bijvoorbeeld of het gevoel van onveiligheid, het gebrek aan thuiszorg of onvoldoende maatschappelijke integratie. De overheid is van mening dat technologie meer voor maatschappelijke problemen kan betekenen dan nu het geval is. Daarom hebben verschillende ministeries samen het interdepartementale programma Technologie & Samenleving in het leven geroepen. Dit programma is gericht op burgers en professionele gebruikers en stimuleert projecten die maatschappelijke vraagstukken helpen oplossen met technologie.
Senter, agentschap van het Ministerie van Economische Zaken, voert het programma-management voor Technologie & Samenleving.

Het deelprogramma Criminaliteitspreventie is een initiatief van:
* het Ministerie van Economische Zaken;
* het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties;
* het Ministerie van Justitie.

Uitgever
SENTER