Biometrie, de technologie

Overheid, burger en biometrie **Criminaliteitspreventie**

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

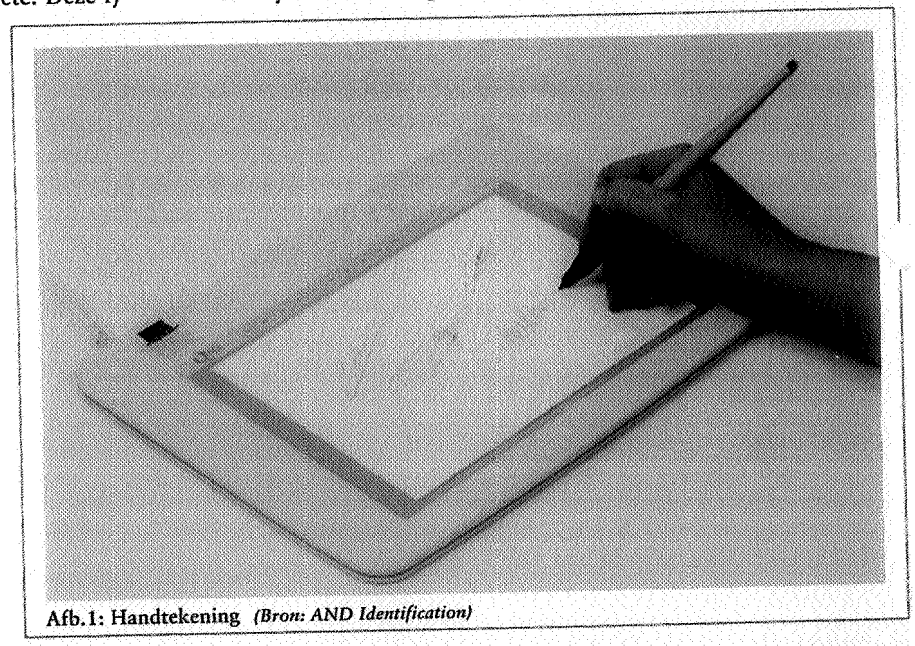
- *Gedragsmatige karakteristieken.* Dit zijn de meetbare aspecten van de manier waarop een persoon handelt of zich uit. Voorbeelden hiervan zijn de stem, de manier waarop iemand een handtekening plaatst en de wijze waarop iemand een toetsenbord bedient. Deze karakteristieken zijn binnen bepaalde bandbreedtes 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)*

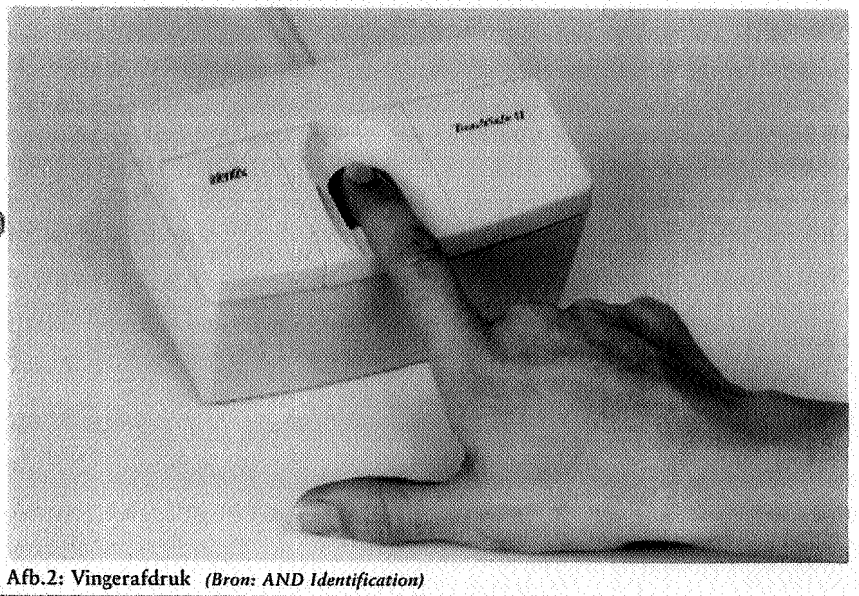
tekening meten, zoals ophalen in de letters etc.
Verder zijn er systemen die met een speciale pen werken, de pen is dan meetinstrument. De handtekening wordt gezet op een z.g. tablet. Hiervoor is al een product op de markt. Een handtekening zetten voor identificatie sluit goed aan bij het huidige maatschappelijk 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.

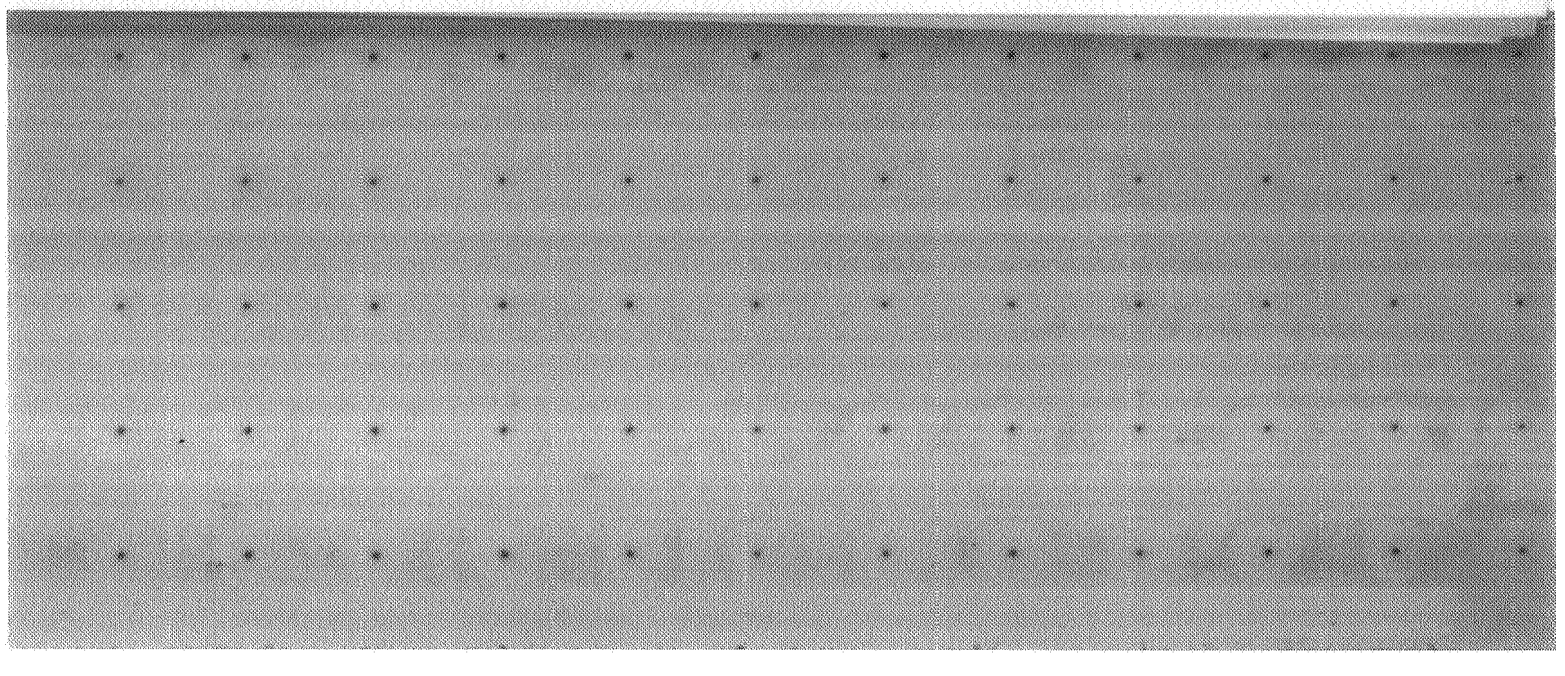


Afb.2: Vingerafdruk *(Bron: AND Identification)*

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 éneiige 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

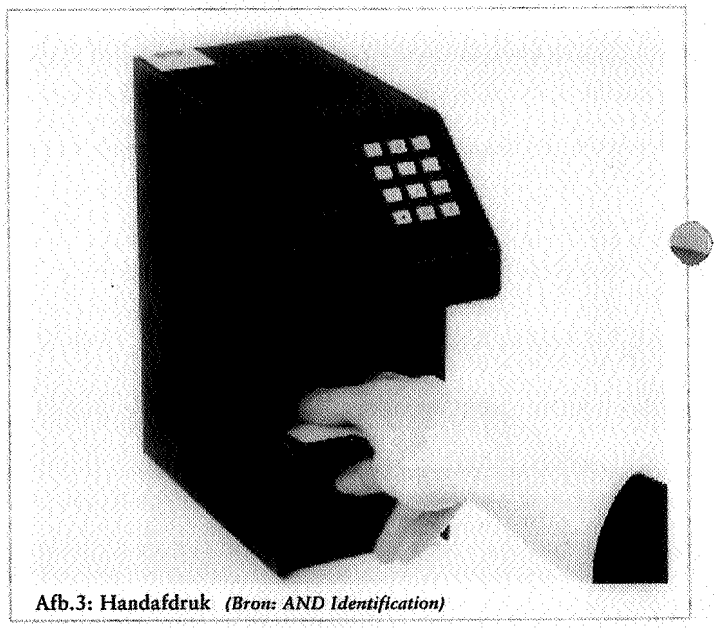
Van alle biometrische technieken biedt gebruik van het oog de beste beveiliging tegen inbreuk. Tegelijkertijd wordt deze techniek als weinig gebruiksvriendelijk ervaren. Bovendien zijn de systemen vrij kostbaar. Het systeem maakt gebruikt van het feit dat de retina aan de achterzijde van het oog een 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.



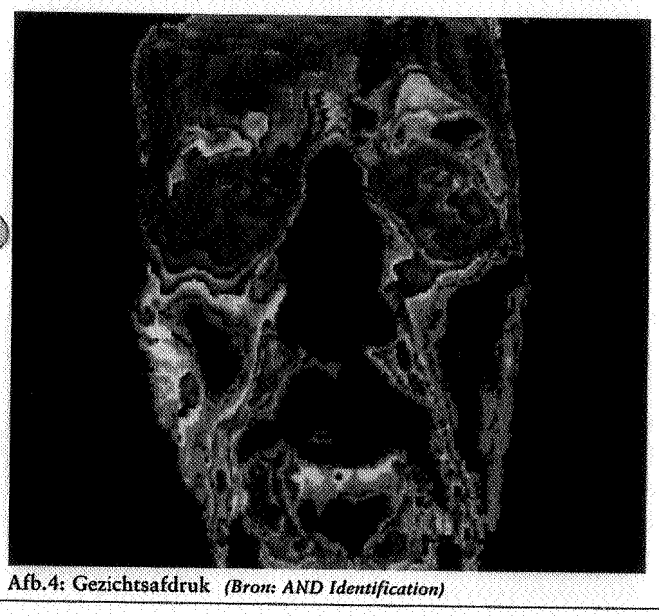
Afb.3: Handafdruk *(Bron: AND Identification)*

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, 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.



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

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.

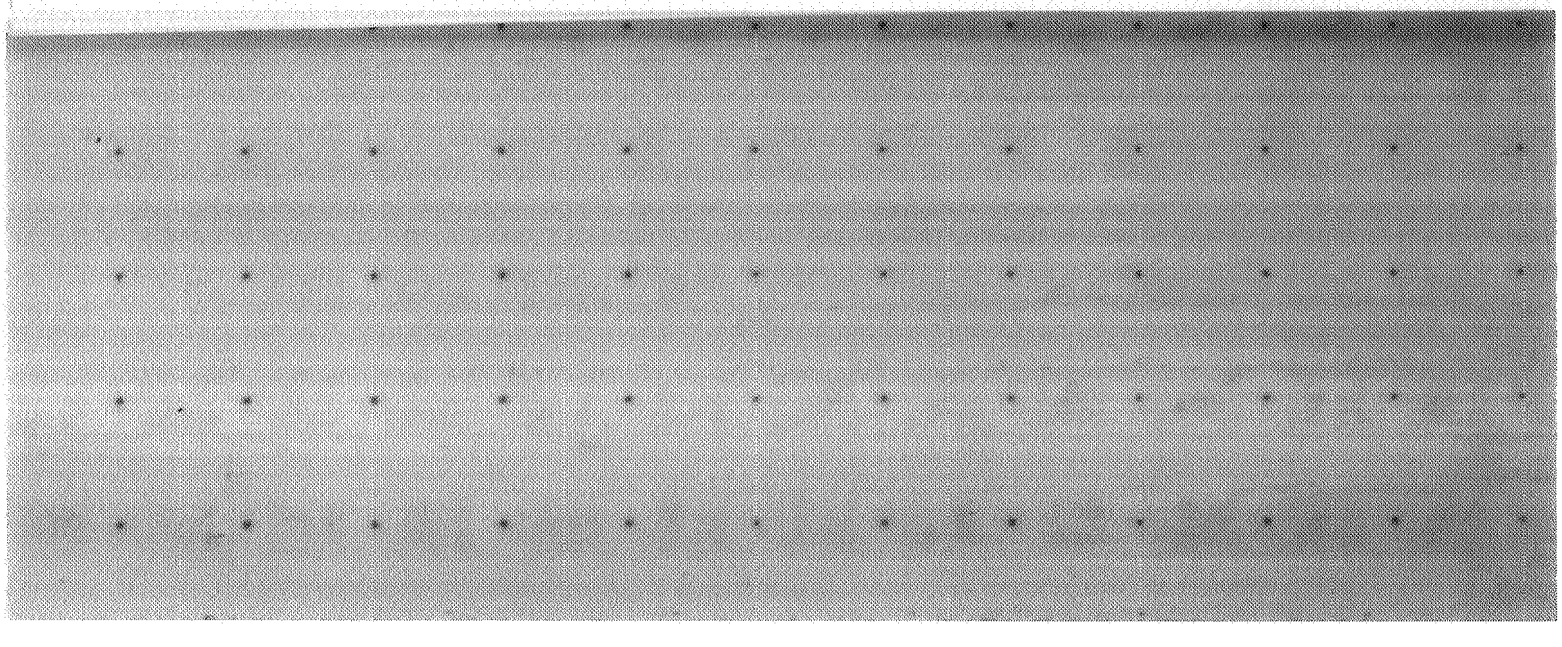
Verschillende niveaus van betrouwbaarheid

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.

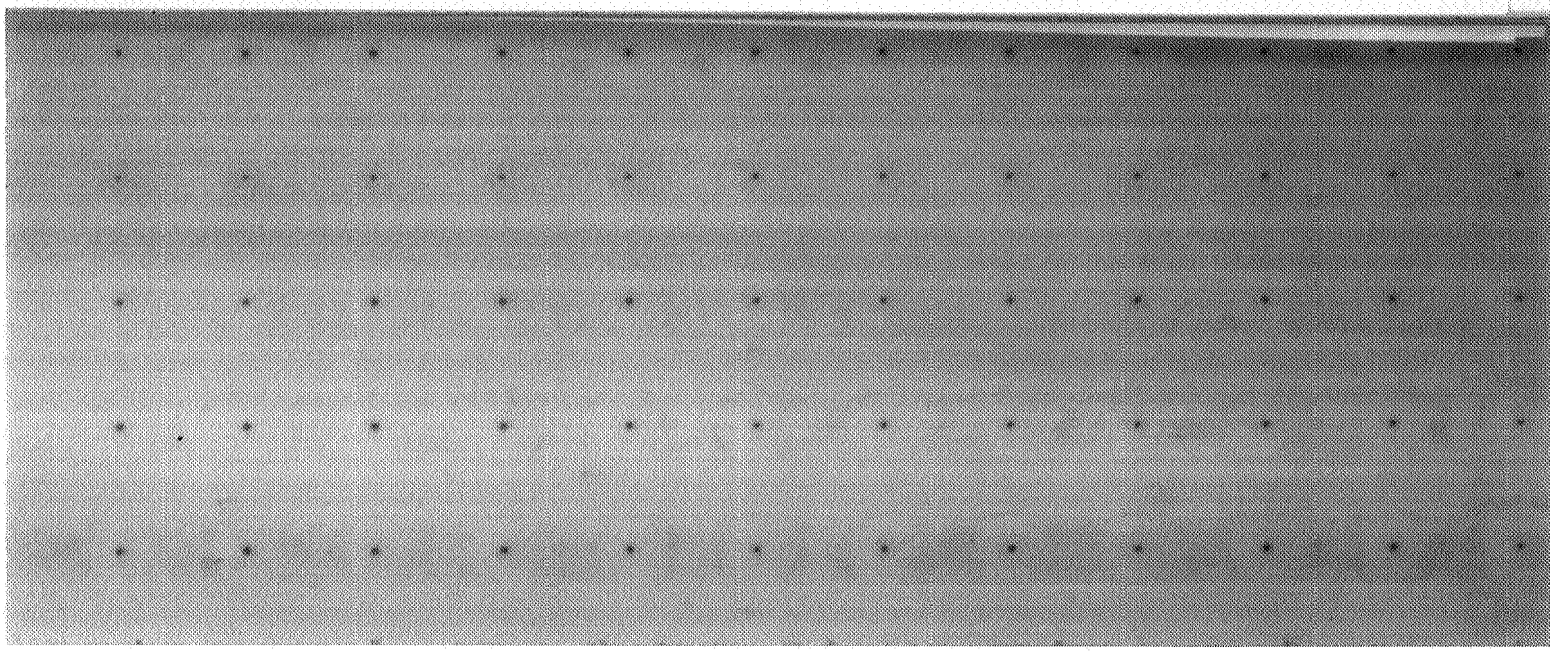
Anonieme biometrie

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,



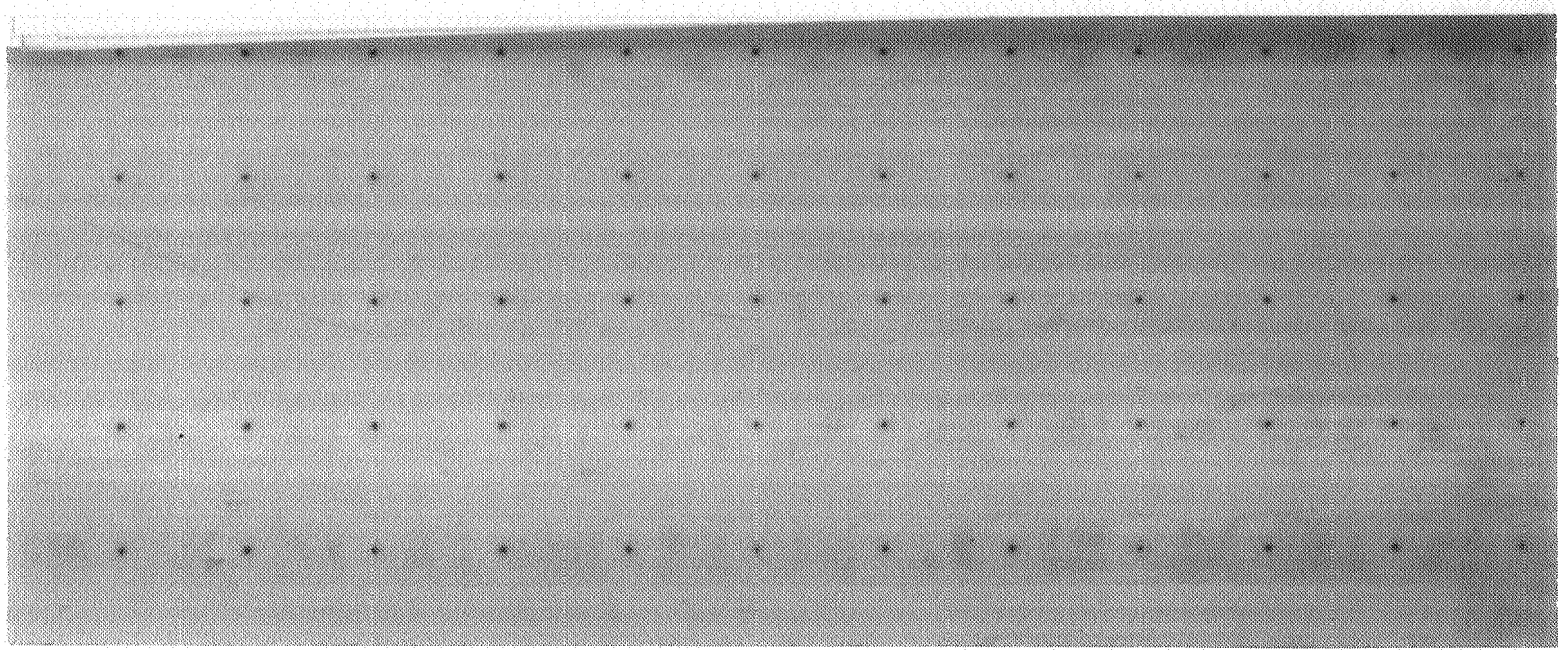
zowel uit een oogpunt van beveiliging als van dienstverlening.[2]

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.

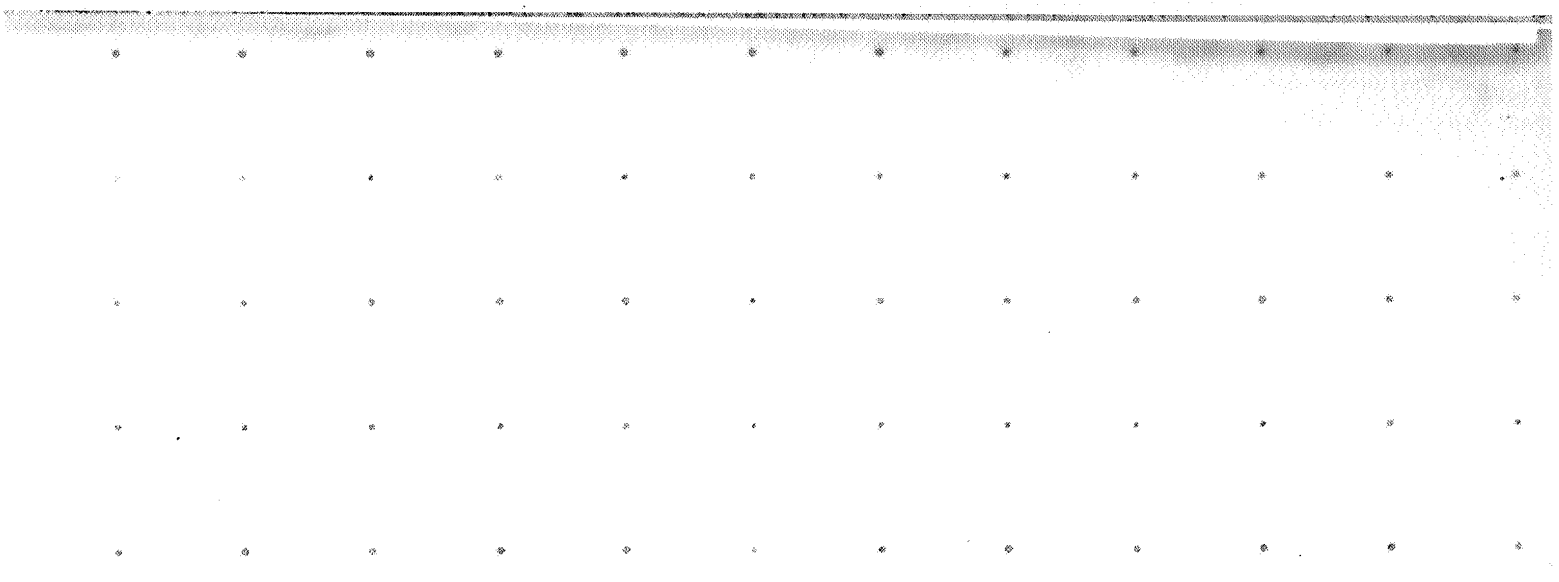
De volgende stap in de technische ontwikkeling is dat ook het leesstation voor een biometrisch kenmerk in de kaart zelf is geïntegreerd. Medio 1998 zijn de prototypen van een flinterdunne vingerafdruklezer, ingebed in een chipkaart, op de markt verschenen. Bij deze opzet komt de vingerafdruk dus noch 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.

[2] 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.[3]

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.

[3] 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

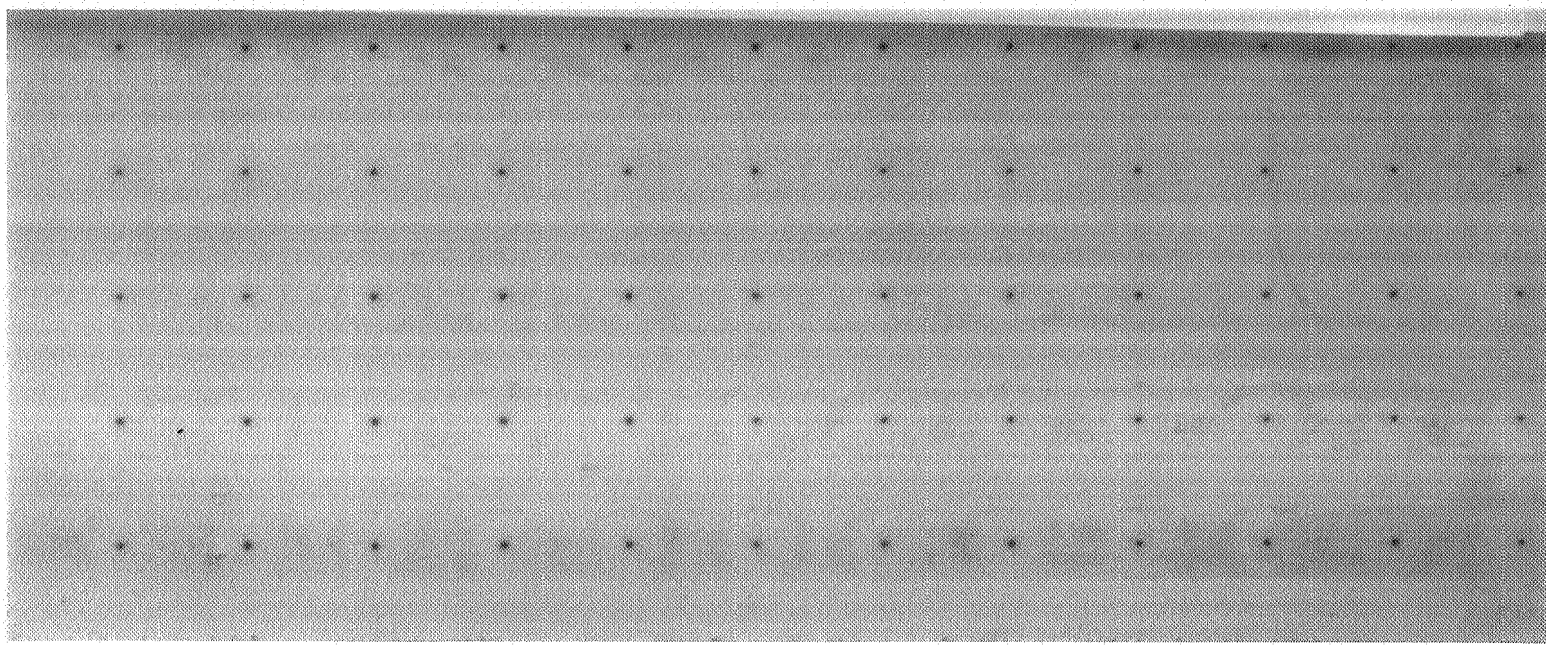
Invoering van biometrie in een systeem brengt organisatorische consequenties met zich mee. Zo is het proces van enrollment zeer arbeidsintensief en dus kostbaar. Ook behoeft de biometrische leesapparatuur het nodige onderhoud. Invoering van een biometrische techniek is dan ook alleen zinvol, wanneer 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.

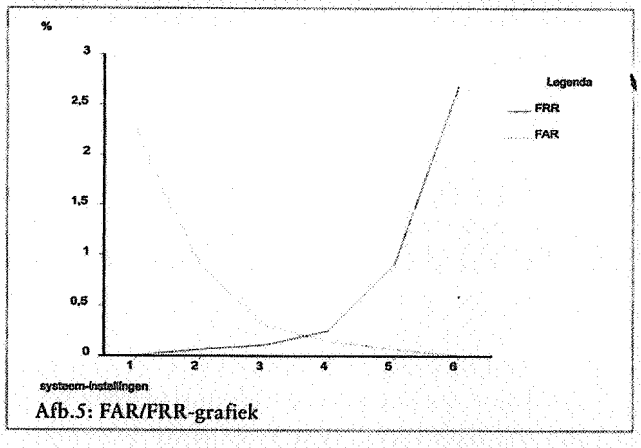
B. Het gebruiksgemak van het systeem

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 acceptante 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.