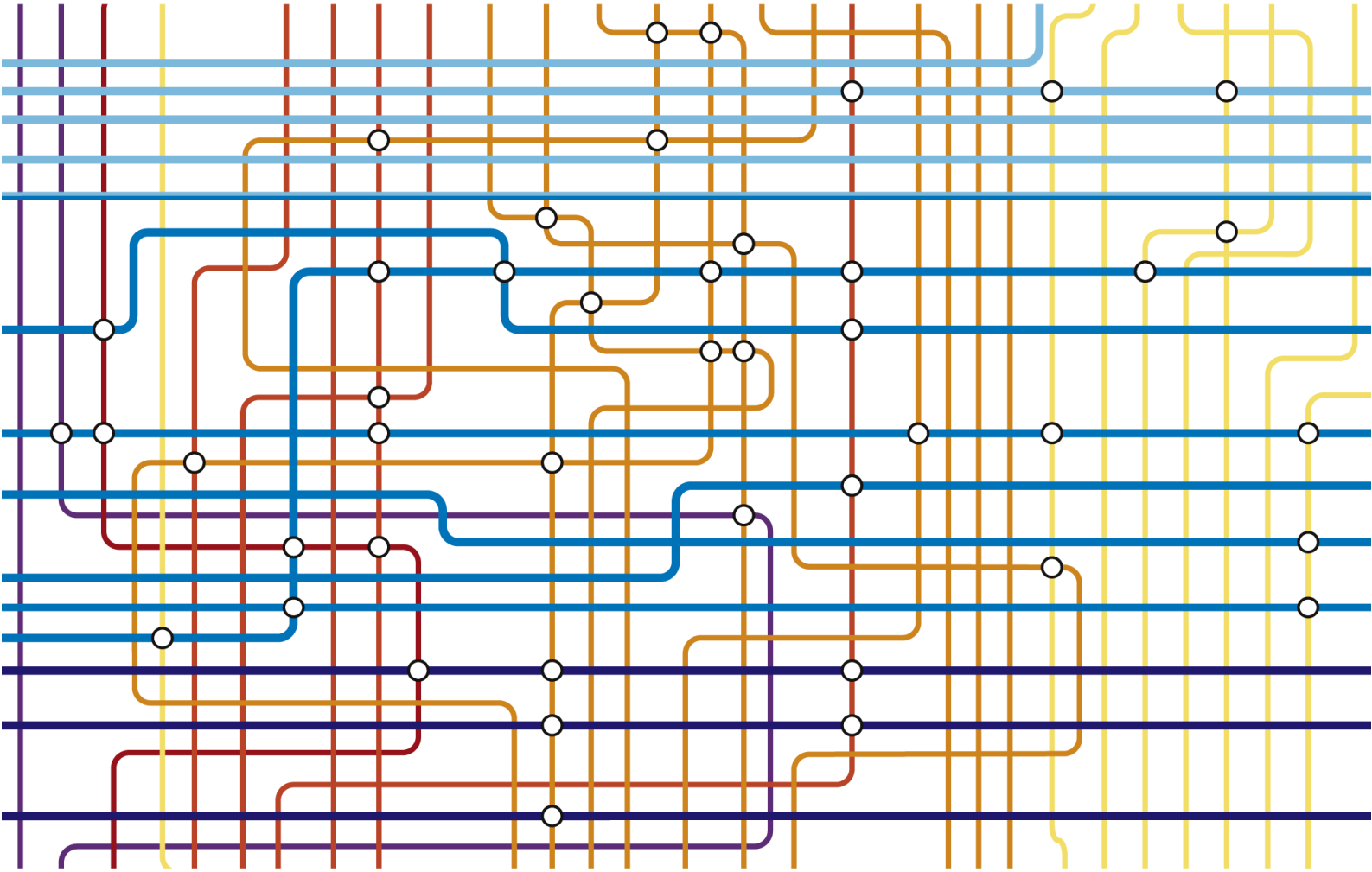
WRR

WETENSCHAPPELIJKE RAAD VOOR HET REGERINGSBELEID



# HET BIOMETRISCH PASPOORT IN NEDERLAND

# CRASH OF ZACHTE LANDING

*Max Snijder*

**WEBPUBLICATIE NR. 51**

***Verkennende studie voor het rapport iOverheid***

De voorliggende studie is opgesteld in opdracht van de Wetenschappelijke Raad voor het Regeringsbeleid, meer specifiek de projectgroep Beleid, Informatie en Technologie (BIT). Het vertrekpunt van het WRR-onderzoek dat voor dit project (in deze en andere studies aangeduid als BIT-project) is uitgevoerd, is de zoektocht naar de rol en verantwoordelijkheid van de overheid bij de inzet van ICT. Daarbij richt het project zich meer in het bijzonder op een tweetal vragen: 1) wat zijn de consequenties van de inzet van ICT voor de relatie overheid-burger en welke tendensen zijn daarin zichtbaar? 2) wat is de betekenis van deze consequenties vanuit de verantwoordelijkheid van de overheid wanneer ze ICT inzet in bedrijfsvoering, beleid en beleidsuitvoering?

Om meer inzicht te verwerven in de dynamiek rondom de ontwikkeling, invoering en het gebruik van ICT in de relatie overheid-burger heeft de projectgroep BIT een aantal empirische studies uitgezet. Daarbij heeft ze de auteurs onder meer gevraagd een aantal beginselen in de analyse te betrekken die als het ware de schragen vormen waarop de relatie overheid-burger in de informatiesamenleving rust. Het betreft de beginselen: keuzevrijheid, identiteit en identificatie, transparantie, effectiviteit en efficiëntie, accountability en privacy.

Om de onderzoeksvragen te kunnen beantwoorden zijn twee typen onderzoek uitgezet bij zowel interne als externe auteurs. De zogenaamde domeinstudies schetsen ontwikkelingen op een breder (beleids)terrein, zoals de zorg, mobiliteit of risicosignalering bij jeugdigen. De zogenaamde black box-onderzoeken geven een weergave van de dynamiek op een veel specifieker gebied of rondom een specifieke toepassing binnen een bepaald terrein, zoals biometrie op het paspoort, het EPD of het Veiligheidshuis. Deze black boxen worden in empirische zin 'opengebroken', om de spelers, interacties, verwevenheden en afhankelijkheden die de ontwikkelingen en keuzes sturen, in kaart te kunnen brengen. Deze bijdrage vormt een van de extern uitgevoerde onderzoeken. Naast de webpublicaties die in het kader van het project BIT verschijnen zal het project naar verwachting begin 2011 resulteren in een WRR-rapport aan de regering en een verkenning. De verkenning vormt, samen met de webpublicaties en de vele interviews die in het kader van het project BIT gehouden zijn, de empirische onderbouwing voor de aanbevelingen in het te verschijnen WRR-rapport dat de titel *iOverheid*' draagt.

De serie webpublicaties omvat studies die in het kader van de werkzaamheden van de WRR tot stand zijn gekomen. De verantwoordelijkheid voor de inhoud en de ingenomen standpunten berust bij de auteurs. Bij het opstellen van het onderhavige rapport is gebruik gemaakt van verschillende informatiebronnen die naar mening van de auteur van voldoende kwaliteit waren. Ook is het rapport afgestemd met de WRR. Dit sluit echter niet uit dat, ondanks het feit dat de auteur alle redelijk van hem te verwachten zorg heeft betracht zich van de juistheid en volledigheid van de geraadpleegde bronnen te vergewissen, één of meer informatiebronnen onjuist en/of onvolledig kunnen zijn dan wel deze informatiebronnen opvattingen kunnen bevatten die afwijken van elders gepresenteerde opvattingen en conclusies. Een overzicht van alle webpublicaties is te vinden op de website van de WRR (www.wrr.nl).

WRR 2010
Omslagillustratie: *Webpagina Zicht op de elektronische overheid*, www.routeplanneregemeente.nl

WRR

WETENSCHAPPELIJKE RAAD VOOR HET REGERINGSBELEID

# HET BIOMETRISCHE PASPOORT IN NEDERLAND:
# CRASH OF ZACHTE LANDING

---

*MAX SNIJDER*

November,2010

**Inhoudsopgave**

## Voorwoord

Op 9 juni 2009 heeft de Eerste Kamer de nieuwe Paspoortwet aangenomen. De wet beschrijft het gebruik van biometrie (gezichtscan en vingerafdruk) in combinatie met reisdocumenten voor verschillende doeleinden, waaronder het bestrijden van identiteitsfraude ('look alike') en opsporing/vervolging. Daarvoor zal een centraal biometrieregister worden aangelegd. De schaal waarop de biometrie ingevoerd gaat worden is ongekend. Er is tot nu toe geen ervaring waarbij op nationale schaal biometrische gegevens worden afgenomen en geregistreerd. Dit roept vragen op rond de nauwkeurigheid van de techniek, procedures en menselijk handelen, en de daarmee samenhangende risico's. Niet in de laatste plaats is het de vraag wat de (langetermijn-) gevolgen kunnen zijn voor de burgers in hun relatie met de overheid en hoe die in het besluitvormingsproces van de nieuwe Paspoortwet zijn meegenomen.

Hoewel het project BIT zich voornamelijk wil richten op het mesoniveau van de 'Paspoort Black Box', is het onontkoombaar om enkele aspecten op het microniveau van de techniek te behandelen. Immers, op een dergelijke grote schaal kunnen kleine afwijkingen en onzorgvuldigheden leiden tot grote gevolgen voor de werkzaamheid en betrouwbaarheid van het geheel. Ook zal deze studie zich gedeeltelijk richten op het macroniveau van met name de biometrische industrie en de standaardisatie. Dit is noodzakelijk, omdat de biometrische industrie internationaal is georiënteerd en Nederland geen nationale biometrieindustrie heeft.

De studie is dan ook opgebouwd langs de drie lijnen betrokken in het besluitvormingsproces van de nieuwe Paspoortwet, te weten de techniek en het proces; de industrie en de markt; en politiek en beleid. De studie zal eindigen met een aantal conclusies, die micro-, meso- en macroaspecten zullen verbinden. Daarmee zal inzicht ontstaan in de wijze waarop de Nederlandse overheid zich heeft gepositioneerd met betrekking tot de inzet van biometrie als onderdeel van de nieuwe Paspoortwet en hoe de biometrie door overheid en politiek is behandeld in de periode 1999 tot heden.

In dit verband is het van belang te wijzen op een parallel gepubliceerde WRR-studie ten behoeve van het WRR-onderzoek. In deze studie, *Happy Landings? Het biometrisch paspoort als zwarte doos*, geschreven door Vincent Böhre en gepubliceerd als webpublicatie op de website van de WRR, staan de relevante Nederlandse actoren, hun doelen en belangen alsmede hun relaties met andere actoren - waaronder met name de burger - centraal. Aan de hand van een zeer gedetailleerde behandeling van de politieke geschiedenis van het biometrische paspoort in Nederland, worden enkele interessante conclusies getrokken welke hier kort samengevat, in de woorden van Böhre, worden weergegeven.

> *"Opvallend is dat het maatschappelijke debat over de nieuwe Paspoortwet pas in de zomer van 2009 op gang gekomen is, terwijl het politieke debat reeds in 1997 haar startpunt kent. Het gebrek aan maatschappelijk debat kan worden toegeschreven aan een gebrek aan aandacht in de media voor het onderwerp en een vrij geruisloze parlementaire ontiwkkeling. Hierdoor zag het gros van de Nederlandse bevolking én het georganiseerde maatschappelijk middenveld zich in de zomer van 2009 plotseling gesteld voor een nationaal fait accompli: verplichte opslag van vingerafdrukken. Na aanname van de nieuwe Paspoortwet, vond het maatschappelijk debat alsnog in versnelde, verhevigde en (mede daardoor) verjuridiseerde vorm plaats. De algemene strekking van de kritiek op de nieuwe Paspoortwet was (en is) dat door deze wet het recht op privacy van iedere Nederlander met voeten wordt getreden. Bovendien lijkt iedere Nederlander min of meer te worden gedwongen om zich daarbij neer te leggen: zonder geldig biometrisch identiteitsdocument wordt men immers als het ware buiten de maatschappij geplaatst. Van enige vorm van keuzevrijheid (in menselijke zin) is in dit verband geen sprake. Het maatschappelijke proces dat hierdoor 'getriggerd' is heeft onlangs een eerste 'apotheose' bereikt in de vorm van een collectieve dagvaarding van de Nederlandse staat wegens vermeende schending van het recht op privacy. In die zin is de relatie tussen de burger en de Nederlandse overheid door het biometrische paspoort niet alleen reeds veranderd, maar ook op scherp komen te staan, althans in juridische zin."*

Met het oog op deze gedetailleerde rapportage betreffende de parlementaire geschiedenis van het Nederlandse biometrische paspoort, zal het derde deel van deze studie betreffende politiek en beleid zich beperken tot het creëren van inzicht in de wijze waarop de overheid met de biometrische techniek is omgegaan. Omdat biometrie in veel opzichten een onvolwassen technologie is, gaat deze studie nader in op de vraag wat de overheid nu precies van de technologie verwacht en hoe de overheid de voorwaarden schept om deze technologie op een effectieve en verantwoorde manier in te zetten. Er zal worden gekeken naar de formulering van het kernprobleem en de vertaling daarvan naar een programma van eisen, inclusief de implicaties voor het gebruik en inrichting van de techniek, processen en procedures. Daarbij zullen verschillende studies en pilots worden betrokken; hoe deze zijn opgesteld en uitgevoerd, en hoe de resultaten zijn gecommuniceerd ten behoeve van het politieke debat. Het kernprobleem, het bestrijden van 'look alike fraude', zal ook regelmatig aan de orde komen, niet in de laatste plaats omdat de formulering daarvan door de jaren heen meerdere gedaanten heeft gekend.

## Inleiding

In deze studie staat de rol van de techniek – in casu biometrie – centraal. Bij de toepassing van biometrie ten behoeve van het Nederlandse paspoort is het niet alleen een bindende factor tussen burger en overheid, maar ook tussen diverse onderdelen van de overheid zelf. Uit deze studie zal blijken dat de technologie niet alleen maar verbindt in gemeenschappelijke belangen, maar ook juist in discussies (of het ontbreken daarvan) waar tegengestelde belangen op het spel staan. De beoordeling van de techniek en de zich ontwikkelende visie op de toepassing ervan in verband met het biometrische paspoort vormt de kern van deze studie.

Vragen die als een rode draad door de studie lopen zijn de volgende.

a. Wat is de basiswerking van de biometrische technologie en wat is de State of the Art?
b. Hoe ziet het (internationale) landschap van de biometrie-industrie eruit en wat voor invloed heeft die op het biometrische paspoort?
c. Hoe zijn overheid en parlement omgegaan met de technologie en wat is de betrokkenheid geweest van diverse actoren?

Aan de hand van deze vragen, en aan de hand van de gekozen structuur die techniek, industrie en politiek als drie afzonderlijke maar samenhangende delen centraal stelt, zal de studie de lezer leiden door diverse meningen en standpunten geuit door betrokkenen in studies, rapporten, artikelen en interviews.

# DEEL I Techniek en proces

# 1. Biometrie: de techniek

## *1.1 Wat is Biometrie?*

Biometrische kenmerken zijn meetbare patronen van het menselijk lichaam. De bredere term biometrie komt uit de wetenschap van het statistisch analyseren van patronen uit de natuur:

*"het vaststellen van tel-, weeg- of meetbare eigenschappen van levende wezens[1]"*

Het doel daarvan is het onderzoeken van de aard van bepaalde patronen, of juist het ontbreken daarvan. In de context van deze studie wordt met biometrie bedoeld:

*"de geautomatiseerde vaststelling of verificatie van de identiteit van een persoon aan de hand van diens unieke lichaams- of gedragskenmerken."*

Deze studie beperkt zich daarbinnen op de drie belangrijkste biometrische modaliteiten: gezichts-, vingerafdruk- en irisherkenning. Dit is in lijn met het beoogde gebruik van deze drie modaliteiten voor het wereldwijd interoperabele paspoort conform internationale afspraken. De kwaliteit van de biometrie is bepalend voor het goed functioneren van een biometriesysteem. Dat geldt voor alle biometrische modaliteiten. Omdat in de nieuwe Nederlandse Paspoortwet diverse functies aan met name de vingerafdruk worden gekoppeld, zal deze studie zich voornamelijk daar op richten. Dat wil niet zeggen dat er voor de pasfoto en de daaraan gekoppelde gezichtsherkenning geen uitdagingen zouden zijn. Integendeel: het kwaliteitsprobleem bij gezichtsherkenning is wellicht nog groter, omdat de technologie, nog meer dan bij de vingerafdruk, gevoelig is voor veranderende omstandigheden, zoals het ouderdomsproces, variabele positionering van het gezicht en omgevingsfactoren. De problematiek zoals die in deze studie met name aan de hand van de vingerafdruktechnologie wordt beschreven, is dan ook in hoofdlijnen van toepassing op gezichtsherkenning. Omdat irisherkenning vooralsnog niet is

1 Van Dale groot woordenboek van hedendaags Nederlands. Utrecht: Van Dale lexicografie, 1984.

opgenomen in de functionele eisen van de nieuwe Paspoortwet, wordt het hier niet behandeld.

### *1.2 Werking van de biometrische techniek in hoofdlijnen*

Een biometrische vergelijking begint altijd met het opnemen van een plaatje ('image' of 'sample') door middel van een sensor. Voor gezicht en iris wordt het plaatje opgenomen met een camera, voor vingerafdrukken zijn er speciale sensoren. Vingerafdruksensoren kunnen werken op basis van druk of hebben een elektrisch dan wel optisch principe. De plaatjes voor vingerafdruk zijn in grijstinten, voor iris in het bijna-infrarode domein (en daarom ook in grijstinten) en voor gezichtsherkenning in kleur of zwart-wit.

Nadat het plaatje is genomen en goedgekeurd (een slecht plaatje valt moeilijk te analyseren), moeten de biometrische kenmerken worden gevonden en geanalyseerd, om daarna te worden vastgelegd in een digitale code. Dit proces heet 'feature extraction', de digitale code waarin de features (ook wel kenmerken) zijn vastgelegd heet een 'template'.

Om een pesoon automatisch te herkennen, of om zijn identiteit aan de hand van biometrie te kunnen verifiëren, moet er eerst een referentie in het systeem worden opgeslagen. Deze referentie kan dan later gebruikt worden om deze te vergelijken met de biometrische gegevens die worden aangeboden ter verificatie of identificatie. Omdat geen twee opnames van dezelfde kernmerken hetzelfde zijn, moet de software door middel van statistische berekeningen bepalen in welke mate biometrische kenmerken van deze twee plaatjes met elkaar overeenkomen. Het is aan de gebruiker om de drempelwaarden voor een match in te stellen. In de volgende paragrafen wordt dieper ingegaan op de verschillende stappen in dit proces.

De kenmerken voor vingerafdruk worden 'minutiae' genoemd. Deze kenmerken worden al vele jaren gebruikt bij politie, justitie en opsporingsdiensten (o.a. door de recherche). Al deze vingerafdruksystemen doen vingerafdrukvergelijkingen op basis van minutiae en worden daarom 'minutiae matchers' genoemd. Grote nationale

vingerafdruksystemen worden ook AFIS genoemd: 'Automated Fingerprint Identification System'. Deze systemen werken met (soms zeer grote) databases van gedigitaliseerde vingerafdrukken, die vervolgens door middel van geautomatiseerde zoekalgoritmen op basis van minutiae worden doorzocht. In een AFIS worden images van tien vingers per persoon opgeslagen. De laatste jaren worden er ook vingerafdrukalgoritmen ontwikkeld die op basis van de patronen werken, de zogenaamde 'shape matchers'.

### *1.3 Het matchingproces*

Wanneer er een image of template is gegenereerd, moet deze als referentie worden opgeslagen. Dat kan in een database of op een kaart (of token). Het grootste verschil tussen deze twee methoden van opslag is dat er in het ene geval een een-op-veelzoekactie (1:n search) moet worden gedaan en in het andere geval een een-op-eenvergelijking. Dit levert belangrijke verschillen op in de nauwkeurigheid en snelheid van een vergelijking, maar ook in het beheer en management van de data.

Nadat de referentie als image of template is opgeslagen, kan deze worden geraadpleegd om vergelijkingen mee uit te voeren. Om een vergelijking uit te voeren, moet eerst opnieuw een plaatje worden opgenomen van het biometrische kenmerk. Dit is het sample. Vervolgens moeten (weer) de kenmerken worden bepaald en wordt er een template gegenereerd. De opgeslagen referentie wordt dan vergeleken met de persoon die op dat moment zijn/haar biometrische gegevens aanbiedt via een sensor. Omdat de plaatjes op twee verschillende tijdstippen worden genomen en de omstandigheden waaronder deze worden afgenomen nooit identiek zijn, zullen ook de plaatjes, en dus de templates, nooit hetzelfde zijn. Dat betekent dat een vergelijkingsalgoritme in staat moet zijn om de mate van overeenkomst te kunnen meten en daar een statistische uitspraak over moet kunnen doen op basis van een van tevoren vastgestelde nauwkeurigheid. Die wordt geregeld met de zogenaamde drempelwaarde ofwel 'threshold'.

Vanwege de verschillen tussen het sample en de referentie kan er geen vergelijking worden gemaakt wanneer de templates zich in versleutelde toestand bevinden. Er

zou namelijk een verschillend resultaat ontstaan wanneer met dezelfde sleutel twee niet-identieke templates worden versleuteld. Het gevolg is dat een versleuteld biometrisch template of image altijd weer teruggebracht moet worden naar het origineel, alvorens een vergelijking gedaan kan worden. Dit heeft directe gevolgen voor de beveiliging van de data en het vergelijkingsproces, omdat op dat moment de originele template of image aan het systeem wordt blootgesteld en daarmee een risico ontstaat voor de veiligheid van de data en de privacy van de eigenaar ervan. Inmiddels is bewezen dat een template (grotendeels) kan worden teruggevoerd tot het oorspronkelijke plaatje en daardoor geen bescherming kan bieden. Voor de veiligheid van de biometrische gegevens betekent dit dat niet alleen de opslag van de biometrische data aandacht behoeft, maar ook het opvragen van de referentie, het ontsleutelen ervan en het plaatsvinden van de vergelijking[2].

### *1.4 Match en non-match*

Een match of een non-match (een 'ja' of een 'nee') ziet er eenvoudig en resoluut uit, maar op de achtergrond zijn er allerlei gradaties van zekerheid waarin deze 'ja' of 'nee' worden uitgedrukt. Dat kan verschillen van 'ik weet 100% zeker dat deze overeenkomen' tot 'het zou kunnen dat het dezelfde zijn, maar zeker weten doe ik het niet'. Dit kan ook uitgedrukt worden in scores. Al met al komt er veel statistiek bij kijken om uitspraken over een biometrische vergelijking te doen. In het verleden vond dit proces handmatig plaats. Vingerafdrukexperts (ook wel dactyloscopisten genoemd) hadden er een dagtaak aan. Maar ook in moderne geautomatiseerde processen is regelmatig visuele inspectie van een expert noodzakelijk. Wanneer bijvoorbeeld op een 'plaats delict' flarden van vingerafdrukken worden gevonden, kan een zoekactie in een database meerdere hits opleveren. Die moeten dan verder worden geanalyseerd door middel van visuele inspectie door experts, om zodoende toch tot een meest waarschijnlijke match te komen. Ook bij de (semi)geautomatiseerde e-Gates, zoals die tegenwoordig op diverse luchthavens zijn geïnstalleerd om passagiers door middel van biometrie snel de grens te laten passeren, wordt achter de schermen meegekeken om te controleren of er geen fouten worden gemaakt door het biometrische systeem en om in te grijpen mocht een fout

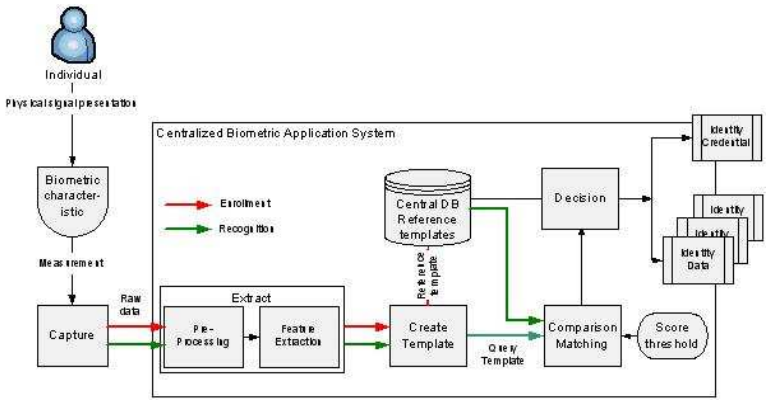
2 Feng and Jain 2010.

zich voordoen. In Europa wordt voor deze e-Gates meestal de gezichtsopname uit het biometrische paspoort gebruikt.

Een uitspraak op basis van een biometrische vergelijking is altijd gebaseerd op kansberekening. De 'life' opgenomen biometrische gegevens zullen namelijk nooit hetzelfde zijn als de gegevens die in het systeem zijn opgeslagen. Er zijn altijd variaties, veroorzaakt door andere omstandigheden (zweethanden, andere lichtval etc.). In dat opzicht wijkt een biometrische vergelijking dus fundamenteel af van bijvoorbeeld een pincode: die klopt, of die klopt niet. Daar zit niets tussen. Het statistisch karakter maakt dat een biometrisch systeem zich heel anders gedraagt dan een gewone database met cijfers en letters. Een zoekactie in een biometrisch systeem levert een resultaat op met een zekere waarschijnlijkheid, een zoekactie in een reguliere database levert het resultaat met een zekerheid op. Een biometrische database werkt op basis van waarschijnlijkheden en marges waarbinnen afwijkingen in bepaalde mate worden geaccepteerd.

Nadat er een biometrische vergelijking heeft plaatsgevonden, komt er een resultaat: een 'ja' of een 'nee'. Deze uitkomst moet worden gecommuniceerd naar het systeem, dat vervolgens bepaalde beslissingen daarop baseert (bijvoorbeeld 'poortje open' of 'poortje dicht', of 'arresteren' of 'laten lopen').

Deze gehele opvolging van acties is het biometrisch proces. Dit proces vindt plaats in het geheel van processen, procedures, technologie en omgevingsfactoren en vormt het biometrisch systeem



*Figuur 1: Het biometrisch proces, www.fidis.net*

### *1.5 Identificatie versus verificatie*

Bij het bepalen van het doel van een biometrisch systeem dient er onderscheid gemaakt te worden tussen het vaststellen van de identiteit ('identificatie') en het verifiëren van de identiteit ('verificatie').

Bij het vaststellen van de identiteit door middel van biometrie wordt niet uitgegaan van een identiteitsclaim. Dit is een uitspraak die een persoon doet over zijn/haar identiteit, bijvoorbeeld door middel van een paspoort, identiteitskaart of alleen verbaal. De meest voorkomende reden om een identiteitsvaststelling aan de hand van biometrie te doen is omdat de identiteitsclaim ontbreekt (bijv. bij een plaats delict) of als onbetrouwbaar wordt beschouwd (bijv. bij een asielaanvraag waarbij onbetrouwbare documenten worden gebruikt). Identiteitsvaststelling aan de hand van uitsluitend de biometrie kan alleen gebeuren door gebruik te maken van een biometrische database, waar biometrie en identiteit aan elkaar zijn gekoppeld. Met een 1:n zoekactie wordt de in de database bekende identiteit gezocht die met de hoogste waarschijnlijkheid bij de gepresenteerde biometrische data hoort.

Deze methode is al vele jaren in gebruik in justitiële omgevingen, zoals opsporing en vervolging, immigratie en bij aanvragen voor asiel. Typerend voor een dergelijk zoeksysteem is dat hoe groter de database wordt, hoe groter de kans is dat er meerdere identiteiten worden gevonden waar de biometrische data overeenkomsten mee vertonen. Om die kans te verkleinen, werken deze systemen op basis van tien vingers. Het is gebruikelijk dat in het geval van meerdere matches er door experts verder handmatig moet worden bekeken wat de meest waarschijnlijke match is. Er zijn internationale systemen die op basis van uitwisseling van biometrische data (bijv. SIS, Verdrag van Prüm) of door raadpleging van een centrale database (zoals het Eurodac en het Europese BMS, onderdeel van het Europese VIS) het mogelijk maken om persoonsgegevens over te dragen wanneer daar om wordt verzocht, bijvoorbeeld bij een internationaal rechtshulpverzoek. Biometrische identificatie kan ook lokaal plaatsvinden, als bijvoorbeeld een deel van een biometrische database wordt gedistribueerd naar een specifieke locatie. Dit is onder andere denkbaar bij

toegangscontrolesystemen, waarbij alleen de biometrische data van geautoriseerde personen worden gedistribueerd naar de betreffende doorgang.

Het verifiëren van een identiteit aan de hand van biometrie is een geheel ander proces. Daarbij vindt er eerst een identiteitsclaim plaats, bijvoorbeeld door middel van een paspoort of smartcard (zie Privium op de Luchthaven Schiphol). Vervolgens wordt de claim gecontroleerd door de biometrie. De biometrische data worden dan één op één vergeleken met de referentie, die veelal is opgeslagen op dezelfde informatiedrager die ook de identiteitsclaim bevat. Dit kan ook gebeuren met een centrale database, maar dan geldt de identiteitsclaim als zoekfunctie voor de database (bijv. naam of paspoortnummer). Dan worden alleen de biometrische data uit dat specifieke record vergeleken. Bij verificatie betekent een match dus dat de identiteitsclaim hoogstwaarschijnlijk correct is. In dat geval leidt de biometrie zelf dus niet tot een identiteitsclaim, maar is de biometrie alleen instrumenteel in het vergroten van de betrouwbaarheid van een eerder gedane identiteitsclaim. Het voordeel van verificatie is dat de biometrische referentie onder de controle van de eigenaar kan blijven, als de biometrische referentie althans niet ook elders is opgeslagen.

De twee hierboven beschreven methoden leiden tot de volgende basisarchitecturen voor een biometrisch systeem:

- centrale identificatie (1:n)
- lokale verificatie (1:1)
- centrale verificatie (1:1 met een pointer/verwijsindex in database)
- lokale identificatie (1:n bijvoorbeeld met een gedistribueerde (deel-) database)

Het maken van een keuze voor een van de bovenstaande architecturen hangt uiteraard af van het Programma van Eisen, ofwel het PvE. Dit is een door de eindgebruiker of opdrachtgever uitgewerkt overzicht van alle eisen en wensen van de verschillende belanghebbenden. Het PvE legt de basis voor de architectuur, techniek

en organisatie. Een PvE is het uitgangspunt voor aanbestedingen en kan variëren van globaal tot zeer gedetailleerd.

### *1.6 'Image Quality'*

Kwaliteitsmeting van de biometrische plaatjes speelt een cruciale rol bij het verbeteren van de nauwkeurigheid en efficiëntie van een biometrisch systeem. Dat geldt voor diverse onderdelen van het biometrische proces.

- Tijdens het registratieproces (als een constante controlevariabele voor initiëren van een nieuwe registratie; het systeem meet de kwaliteit en start automatisch een nieuw capture proces indien de kwaliteit niet voldoende is).
- Voor het onderhoud van de databases (het updaten van de geregistreerde samples).
- Voor organisatiebrede controle op de waarborging van de kwaliteit.
- Voor het initiëren van kwaliteitsgestuurde verwerking van biometrische samples.

Als de kwaliteit kan worden verbeterd, hetzij door het ontwerp van de sensor, door het ontwerp van de user interface of door conformiteit met geldende standaarden, kunnen betere prestaties worden gerealiseerd. Voor kwaliteitsaspecten die geen vast onderdeel van het ontwerp uit kunnen maken (bijv. mate van medewerking van de te registreren persoon, fysieke toestand van de af te nemen biometrische karakteristieken) is de mogelijkheid tot een kwaliteitsanalyse van een live sample noodzakelijk. In eerste instantie is dat nodig om een eventuele herregistratie van een gebruiker te initiëren, maar ook voor de real-time selectie van het beste sample en een op kwaliteitscriteria gebaseerde initiatie van de verschillende verwerkingsprocessen.

Biometrische kwaliteitsanalyse is een technische uitdaging, omdat kwaliteitsaspecten invloed hebben op de prestatiegevoeligheden van een of meerdere biometrische

matchers. Het Amerikaanse NIST[3] heeft dit probleem in 2004 geadresseerd, toen zij het NIST Fingerprint Image Quality (NFIQ) algoritme introduceerde. NFIQ is een instrument om de kwaliteit van vingerafdrukken te meten. Het is geïmplementeerd als open-source software en is thans in gebruik binnen de Amerikaanse overheid en bij diverse commerciële toepassingen. NFIQ is een automatisch lerend algoritme en de belangrijkste innovatie ervan is dat het kwaliteitswaarden kan leveren die een directe voorspellende waarde hebben met betrekking tot de te verwachten prestaties bij een vergelijking. NFIQ is beschikbaar als een publiek verkrijgbare referentie.

De kwaliteit van het image heeft een grote invloed op met name grootschalige biometriesystemen. Goede prestaties kunnen alleen worden verkregen wanneer zowel het geregistreerde image (de referentie) als het te verifiëren image van goede kwaliteit is. Een uniforme meetmethode, die kan voorspellen hoe groot de kans is dat een latere verificatie succesvol zal zijn, is daarvoor nodig. Deze meetmethode moet aan de volgende eisen voldoen.

- De meetmethode moet gebaseerd zijn op een consistent en algemeen geaccepteerd criterium voor de definitie van 'goede kwaliteit'.
- De meetmethode moet in staat zijn om de prestaties te voorspellen bij gebruik van vergelijkingssoftware van meerdere leveranciers.
- De methode moet de mogelijkheid hebben het meest bruikbare plaatje te kiezen tijdens het registratieproces (bijv. het vermogen om te bepalen of het de moeite waard is om een afdruk opnieuw te nemen in het geval van een lage kwaliteit van de afdruk).
- Het leveren van een indicatie van de mate waarin de kwaliteit van de afdruk de plaatsing van de minutiae beïnvloedt.

Partick Grother, biometrie-expert van NIST, zegt over kwaliteit verder het volgende.

*"Lowering the quality acceptance thresholds at the point of fingerprint capture might solve the FTE (Failure to Enrol) en FRR (Fasle Rejct Rate) issue, but will definitely lead to a significant lower performance of the central system. This will*

3 Het federale technologieagentschap van de VS, dat samenwerkt met de industrie om technology, evaluaties and standaards te ontwikkelen en toe te passen.

*result in higher costs (because of exception handlings and corrections of mistakes) and a lower return on investment for the system as a whole, from a cost of ownership point of view, but also regarding the contribution that the system should bring to enhance the security of the overall system."*[4]

### *1.7 Prestaties: FRR, FAR en FTE - een kwestie van afregelen*

De belangrijkste statistische eenheden die bij een biometrische vergelijking worden gebruikt om de nauwkeurigheid en prestaties mee uit te drukken zijn de volgende.

| afkorting | Term | Betekenis |
|---|---|---|
| FAR of FMR | False Accept Rate of False Match Rate | De kans dat het systeem ten onrechte een aangeboden life sample als overeenkomstig ziet met een in het systeem opgeslagen referentie. Het meet het percentage van ten onrechte 'herkende' life samples. |
| FRR of FNMR | False Reject Rate of False Non-Match Rate | De kans dat het syseem ten onrechte een aangeboden life sample niet herkend. Het meet het percentage van geldige inputs (i.e. input van personen die zeker in het systeem zijn geregistreerd) die desondanks ten onrechte zijn verworpen. |
| FTE | Failure To Enrol | Biometrische samples die correct zijn afgenomen, maar die door het systeem niet kunnen worden opgeslagen (bijv. omdat de kwaliteit niet voldoet of omdat het systeem al een soortgelijke dataset in de database aantreft). |
| FTA | Failure To Acquire | Het percentage mislukte pogingen tot het opnemen van een biometrische karakteristiek. Dit kan veroorzaakt worden door nadelige omgevingsfactoren, door een slechte kwaliteit of |

4 In Wilson et al. 2003.

| | | |
|---|---|---|
| | | algehele afwezigheid van het fysieke karakteristiek, of door tegenwerking van de persoon. |
| TAR | True Accept Rate | Het percentage correcte herkenningen. |
| TRR | True Reject Rate | Het percentage terechte niet-herkenningen, veroorzaakt doordat de gepresenteerde biometrische gegevens van een andere persoon zijn dan de gegevens waarmee deze worden vergeleken. |

*Figuur 2: Overzicht meeteenheden voor biometrische prestaties, http://www.eubiometricsgroup.eu/*

Los van hun technische betekenis representeren de hierboven genoemde meeteenheden belangen van verschillende gebruikers van biometrische systemen. De eisen voor veilgheid zullen met name om een lage FAR vragen. Gebruikersgemak is daarentegen meer gediend bij een lage FRR. Het lastige hierin is dat een lage FAR betekent dat de FRR omhooggaat. In grote lijnen betekent dat: hoe veiliger het systeem, hoe minder gebruikersvriendelijk. Het uitbalanceren van deze systeemeigenschappen wordt gedaan door het instellen van de drempelwaarde voor het al of niet accepteren van een match of non-match. Bij een lage FAR moeten er veel overeenkomsten gevonden worden. Een lage FRR vraagt al snel om een lagere acceptatiedrempel.

Wanneer de projectleiding van een biometrisch project alle eisen en wensen van de verschillende belanghebbenden heeft uitgewerkt, ontstaat er een Programma van Eisen. Een goed PvE moet een nauwkeurige weergave zijn van de geconsolideerde functionele eisen en het moet duidelijk zijn wat de prioriteiten zijn. Immers, een PvE waarin tegenstrijdige eisen staan leidt tot onduidelijkheid in de te maken keuzes met betrekking tot de techniek, processen en procedures.

Bij het opstellen van de eisen voor de prestaties van het biometrische systeem kan het bepalen van de hoogte van de drempelwaarden een ware onderhandeling zijn

tussen verschillende belanghebbenden. Zo zal de verantwoordelijke voor de beveiliging van grenspassages veel hechten aan een lage FAR, terwijl de operator van een luchthaven zich eerder zorgen maakt over een te hoge FRR. Mensen die ten onrechte niet worden herkend gaan klagen en worden ontevreden. Naast een slecht imago zal dat ook extra werklast opleveren, omdat deze mensen extra aandacht nodig hebben.

Bij het aanvragen van een paspoort op een drukbezochte buitenlandse consulaire post maakt men zich vooral zorgen over de FTE en FTA. Mensen bij wie het niet lukt om de biometrische gegevens af te nemen staan langer in de rij en kunnen gaan klagen. Vaak komen zij van ver en is het geen optie om hen onverrichter zaken terug te sturen. Daarbij komt dat de oorzaak van een weigering onderzocht moet worden, hetgeen ook tijd kost.
Dus als we het gebruikersgemak en de doorlooptijd van een biometrische registratie willen verhogen, dan zullen we het systeem zodanig willen afstellen dat de FRR niet te hoog is. Maar dat houdt automatisch in dat de FAR hoger zal zijn, omdat het systeem minder kritisch zal oordelen en ook bij relatief weinig overeenkomsten aan zal geven dat er voldoende gelijkenis is. Daarmee neemt de nauwkeurigheid van de biometrische vergelijking dus af en zal de TAR lager zijn.

De TAR en TRR zijn essentiëel voor het bepalen van de veiligheid en betrouwbaarheid van het biometrische systeem. Om deze waarden te meten is een nauwkeurige en permanente controle van zowel de geslaagde als mislukte verificaties en identificaties noodzakelijk. Dat vereist uitgebreide logging en interpretatie van de gebeurtenissen. Dit is arbeidsintensief en niet eenvoudig, en daarom een kostenverhogende factor die men vaak buiten beschouwing laat. Echter, zonder deze metingen zijn de echte prestaties van een biometrisch systeem niet te bepalen.

Voor het verkrijgen van een lage FAR én FRR is de kwaliteit van de gebruikte biometrische images van groot belang. Maar om dat te verkrijgen dienen er bepaalde investeringen te worden gedaan. Het verkrijgen van hoogwaardige kwaliteit biometrie kost meer tijd, vraagt om betere apparatuur, beter opgeleid baliepersoneel en strak afgestemde omgevingsfactoren.

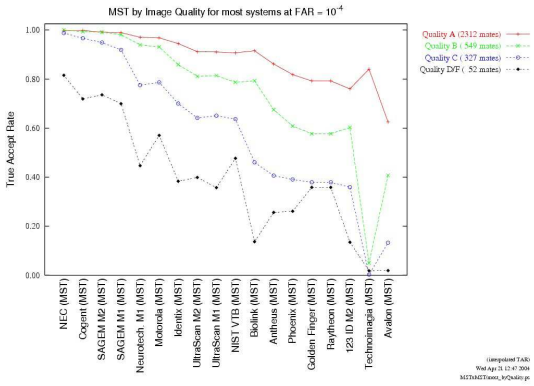
Bij een lage kwaliteit van de biometrische data kan men bij een 1:n zoekactie de volgende prestaties verwachten al naar gelang de instelling van de drempelwaarden.

- Drempelwaarde hoog: een lage match-rate, omdat er te weinig betrouwbare overeenkomsten zijn met opgeslagen data. Dit levert een hoge FRR op.
- Drempelwaarde laag: een hoge, maar onbetrouwbare match-rate, omdat er veel data zijn die enige overeenkomst vertonen. Dit levert een hogere FAR/FMR op en een lagere TAR. Om dat te compenseren zullen de biometrische data dus handmatig moeten worden gecontroleerd, hetgeen het systeem langzaam en kostbaar maakt.

In andere woorden: een lage kwaliteit van de biometrische data maakt het systeem onbetrouwbaar en daarom minder efficiënt. Afhankelijk van de eisen is een lagere kwaliteit al of niet acceptabel. De volgende paragraaf gaat daar veder op in.

### *1.8 Invloed van kwaliteit op de nauwkeurigheid van de matcher*

Het is bekend dat biometrische plaatjes van een slechte kwaliteit moeilijk zijn om te matchen. Bij grootschalige toepassingen is dit een factor die in de praktijk moeilijk is te beheersen. De effecten van kwaliteit zijn duidelijk en dramatisch, zoals blijkt uit het figuur hieronder, onderdeel van de resultaten van de NIST Vendor Fingerprint Technology Evaluation (FpVTE) uit 2003. Het National Institute for Standards and Technology (www.nist.gov) is in Amerika gevestigd en is sinds jaren het meest toonaangevend testinstituut in de wereld met betrekking tot biometrie.




*Figuur 3: Grafiek uit Wilson et al. 2003*

Uit de figuur valt af te lezen dat biometrische systemen bij plaatjes van goede kwaliteit zonder uitzondering beter presteerden dan bij slechte kwaliteit van de plaatjes.

Volgens NIST zijn deze bevindingen belangrijk om verschillende redenen. In de eerste plaats kunnen en moeten operationele procedures worden gebruikt om de kwaliteit van de vingerafdrukken te controleren. Ten tweede kunnen systeemarchitecten op basis van deze bevindingen modellen ontwikkelen die het effect van verschillende vingerafdrukkwaliteit op de prestaties van de matcher in kaart brengen. Hierdoor kan een voorspelling worden gedaan over de prestaties en kosten van het systeem. Ten derde, systemen kunnen vingerafdrukkwaliteit gebruiken om de betrouwbaarheid van de zoekfunctie te voorspellen (lage kwaliteit leidt tot hogere FNMR). Opgemerkt moet wel worden dat de relevantie van tests beperkt is, waneer de distributie van de vingerafdrukkwaliteit niet bekend is. Bovendien kunnen de uitkomsten van tests bijzonder variëren als de vingerafdrukkwaliteit niet onder strikte controle staat.

De FpVTE bevestigt dat slechte kwaliteit van vingerafdrukken de nauwkeurigheid van het systeem in hoge mate reduceert. Voor alle geteste systemen gold dat hoge kwaliteit images een veel hogere nauwkeurigheid opleverde dan bij lage kwaliteit. Sommige systemen waren zelfs uitzonderlijk gevoelig voor lage kwaliteit.[5]

### *1.9 Spoofing*

Spoofing (het namaken van andermans biometrie) is nog steeds een van de grootste uitdagingen voor de producenten van biometrische producten. Het namaken van andermans vingerafdruk is een kwestie van minuten en kan met zeer eenvoudige

5 Zo gaf Technoimagia bij een FAR van 0,01% een spreiding aan van een TAR van 82% bij de hoogste kwaliteit images tot maar liefst 2% voor de laagste kwaliteit. Volgens die test kon dat systeem bij lage kwaliteit dus bijna niet meer functioneren. Het systeem van NEC presteerde op dit punt het beste en haalde bij dezelfde FAR 99,8% bij de beste tot 84% bij de slechtste kwaliteit afdrukken. Dat betekent nog altijd een FRR van maar liefst 16%, vrijwel uitsluitend veroorzaakt door een slechte kwaliteit van de vingerafdrukken. Cogent en Sagem (resp. 2de en 3de plaats) kwamen bij een slechte kwaliteit tot scores van rond de 75%, een FRR van 25%.

middelen.[6] Het is mogelijk om een nep-vingerafdruk dermate subtiel te maken dat het nauwelijks met het blote oog waarneembaar is. Hoewel de industrie regelmatig claimt de oplossing daarvoor te hebben gevonden, is er nog steeds geen enkel product op de markt dat die claim voldoende kan waarmaken.

Hoewel iets minder eenvoudig, geldt hetzelfde voor de iris. Huidige camera's kunnen maar met veel moeite bewerkte contactlenzen onderscheiden van echte ogen. Sommige camera's nemen al genoegen met een simpele foto van een oog, geplakt op een contactlens of glazen oog. Wel zijn er camera's die in staat zijn om een foto van het oog te detecteren. Met gezichtsherkenning is het al niet veel anders. Sommige software accepteert een eenvoudige foto, bij andere is het nodig om bijvoorbeld via een laptopbeeldscherm bewegende beelden voor te houden. Weer andere gezichtsherkenningsprodukten combineren het gezicht met de stem.
De risico's van spoofing zijn inmiddels alom bekend. Vanuit de toepassing beschouwd zijn er drie risicoprofielen:

1. biometrietoepassingen onder direct toezicht (supervised);
2. biometrietoepassingen onder gedeeltelijk toezicht (semi-supervised of semi-unsupervised);
3. biometrietoepassingen zonder toezicht (unsupervised).

Bij het ontwerpen van een biometrische toepassing moet hier rekening mee gehouden worden. Zoals met elke techonolgie: 100% betrouwbaarheid bestaat niet. Er zijn alleen wel grote verschillen tussen de biometrische technieken in de eenvoud waarmee ze kunnen worden geïmiteerd en/of gemanipuleerd en de mate waarin dit door visuele of geautomatiseerde inspectie detecteerbaar is. Een eenvoudig na te maken biometrie hoeft geen probleem te zijn wanneer het in een gecontroleerde omgeving met direct toezicht wordt gebruikt. Voorwaarden daarbij zijn dat het toezicht vakkundig is en dat de processen en procedures ingericht zijn op de visuele inspectie. Een moeilijk na te maken biometrie in een gecontroleerde omgeving levert relatief laag risico op.

6 Zie in dit verband bijvoorbeeld http://www.youtube.com/watch?v=VZT1CVWal2w http://www.youtube.com/watch?v=-H71tyMupqk.

### *1.10 De relativiteit van resultaten uit testlaboratoria*

Een belangrijke kanttekening die NIST plaatst bij het interpreteren van tests is dat de nauwkeurigheid bij gecontroleerde testdata significant hoger ligt dan bij data vanuit een operationele situatie.

In veel gevallen wordt voor de prestaties van biometrische technologieën (zoek- en vergelijkingsalgoritmes) verwezen naar testresultaten van NIST, wereldwijd het meest gezaghebbende testinstituut voor biometrie. Vaak wordt dan geen rekening gehouden met de geconditioneerde omstandigheden en testdata van dergelijke tests. NIST gebruikt veelal gevalideerde databases, waar de algoritmes van allerlei leveranciers op worden losgelaten. Deze testdatabases zijn samengesteld onder andere op de kwaliteit van de afdrukken en het type sensor waar de afdrukken mee zijn afgenomen. Overigens zijn de databases publiek toegankelijk, wat de interessante situatie oplevert dat leveranciers van biometrische software eerst hun producten afstemmen op die databases om pas daarna een test door NIST te laten uitvoeren. Dat proces wordt ook wel training genoemd. Tests op basis van operationele databases[7] zijn dus in principe interessanter om prestaties van biometrische systemen te kunnen voorspellen dan tests waarbij leveranciers van tevoren hun algoritmes kunnen trainen en waar de soort en kwaliteit van de data bekend zijn.

Bij het interpreteren van de uitkomsten van een laboratoriumtest moet dus altijd gekeken worden naar het type database dat is gebruikt. Deze is namelijk niet altijd representatief voor een bepaalde toepassing. NIST gebruikt dan ook meerdere testdatabases met verschillende soorten vingerafdrukken (meerdere kwaliteiten en meerdere methoden: gerold, slaps, optisch, latent). Daardoor kan een klant tests laten uitvoeren op basis van een database die het meest overeenkomt met het soort vingerafdrukken dat hij vanuit zijn eigen toepassing kan verwachten. Bij een nog niet bestaande toepassing, waar nog geen ervaring mee is opgedaan en waar geen voorbeelddata van bestaan, is het dus een kwestie van inschatten of een bepaalde test relevant is of niet. Om die inschatting zo betrouwbaar mogelijk te kunnen doen zal de klant eerst diverse aspecten van zijn toepassing moeten ontwerpen (functioneel,

7 Zoals de in de FpVTE gebruikte IDENT en IAFIS databases.

procedureel, omgeving, bediening etc.) en goed gedocumenteerde proeven moeten uitvoeren om tot een representatieve dataset te komen. Die dataset kan dan als basis fungeren voor het kiezen van een referentiedatabase.

### *1.11 Operationele factoren*

In 2003 heeft het NIST een grootschalige test uitgevoerd met betrekking tot de prestaties van grote vingerafdrukdatabases, de Fingerprint Vendor Technology Evaluation 2003 (FpVTE).[8] Naast het belang van rekening houden met de geconditioneerde omstandigheden en testdata wijst het NIST op het belang van de invloed die operationele factoren hebben op de kwaliteit en prestaties van een biometrisch systeem. Het NIST zegt hierover het volgende.

*"When discussing the implications of the FpVTE results for operational systems, several issues need to be emphasized:*

- *Real world operational results for a system may be better or worse than the results reported here. Differences may arise from factors such as the operational environment, sources and types of fingerprint data, capture devices, operators and their training, hardware and software architecture and implementations, throughput requirements, and gallery size. One important conclusion of FpVTE is that such factors have a clear but complex effect on the performance of fingerprint systems.*
- *Operational systems are likely to use different operating points than are cited here, with correspondingly different error rates.*
- *Operational systems can be tuned to maximize performance given a particular concept of operations.*
- *Many systems have the ability to trade off accuracy for throughput: different throughput requirements will result in different levels of accuracy. Very high throughput requirements may be attained through a drop in accuracy.*
- *System cost must always be considered for operational systems."*[9]

8 Wilson et al. 2003.
9 Wilson et al. 2003.

Een ander niet te onderschatten aspect van het testen van biometrische systemen met gebruikmaking van grote databases is dat er inherente fouten (zogenaamde 'ground truth errors') kunnen zitten in de validatie van testdatabases, waardoor er fouten ontstaan die ten onrechte aan het biometrische systeem worden toegeschreven. In het geval van de hier besproken FpVT zijn deze fouten (ook wel 'mating erros') gecorrigeerd voordat de scores werden vastgelegd. Zeker wanneer er getest wordt tegen zeer kritische FAR's en FRR's is het belangrijk dat deze 'mating errors' worden voorkomen.

Overigens is het opstellen van referentiedatabases een bijzonder arbeidsintensief en gespecialiseerd proces. Elke vingerafdruk moet afzonderlijk worden beoordeeld en in een bepaalde categorie worden ingedeeld. Om met een test een relevante en betrouwbare uitspraak te kunnen doen over prestaties van een biometrisch algoritme op grote schaal, is een referentiedatabase met tienduizenden tot miljoenen vingerafdrukken nodig. Dit geldt voor elke modaliteit, dus ook voor gezichtsherkenning en irisherkenning. Om vervolgens een testdatabase geaccepteerd te krijgen door alle spelers in de markt moet er op verschillende fronten veel gebeuren. Ten eerste moet de industrie de referentiedatabase accepteren en haar producten daarop afstemmen (dit betekent productontwikkeling). Ten tweede moeten, om internationale consensus (en dus interoperabiliteit) te krijgen, uniforme testtools worden ontwikkeld, die waar dan ook in de wereld op dezelfde wijze worden ingezet. In de derde plaats moeten de overheden in grote eensgezindheid besluiten tot het gebruiken van dezelfde referentiedatabase en bijbehorende testtools. Zo ontstaat er een kritische massa waardoor de industrie gedwongen wordt haar producten aan te passen. Tot slot moeten de onafhankelijke testlaboratoria investeren in het ontwikkelen van testprotocollen en procedures, zodat overheden dit gespecialiseerde testwerk kunnen uitbesteden.

Bij vingerafdruksensoren speelt nog een ander probleem. Sensoren die gebaseerd zijn op contact tussen de vinger en de sensor (waarbij de uitgeoefende druk op de sensor een patroon veroorzaakt) leveren door een zekere vervorming van de vinger een ander soort plaatje op dan bijvoorbeeld optische sensoren, waarbij geen druk op de sensor hoeft te worden uitgeoefend. Voor het beoordelen van de prestaties is het dus

ook belangrijk om te weten welke sensoren er zijn gebruikt. Het probleem bij deze tests is dat nooit het volledige scala aan factoren kan worden meegenomen, omdat dat in een laboratoriumsituatie praktisch onhaalbaar is. Om die reden is het grondig testen van de apparatuur in operationele omstandigheden zeer belangrijk. Voorwaarde daarbij is dat alle onderdelen en omstandigheden van het gehele biometrische proces tot in details worden gedetermineerd en onafhankelijk getest.

### *1.12 De kwaliteit van een biometrisch systeem*

Pas wanneer het gehele scala aan factoren wordt meegenomen kan er een uitspraak worden gedaan over de zogenaamde end-to-end prestaties van het systeem. Dat zal in de praktijk moeten worden getest, waarbij al deze factoren onafhankelijk én in relatie tot elkaar in beschouwing moeten worden genomen. Daarbij spelen tenminste de volgende factoren een rol.

- Het gebruik van sensoren van meerdere leveranciers.
- De vaardigheden van baliepersoneel.
- De leercurve van de gebruikers.
- De fysieke omstandigheden waarin de biometrische apparatuur zich bevindt (lichtinval, vochtigheid, stof, positionering sensoren/camera's etc.).
- De wijze waarop de software is ingesteld.
- De kwaliteit van het onderhoud.
- De ergonomie van de technische opstelling.

Pas als al die factoren worden meegnomen kan een uitspraak worden gedaan over de prestaties van het systeem als geheel en kunnen oorspronkelijke doelstellingen getest worden. Dit vraagt een zeer systematische en modulaire opzet van het functionele en technische ontwerp.

Het is deze veelheid aan beïnvloedende factoren waardoor de laboratoriumtests slechts een relatieve betekenis hebben. Bureaustudies zijn meestal al helemaal onbruikbaar en kunnen hooguit een grove richting geven. Met name dient men zich te realiseren dat in een operationele omgeving de prestaties vanwege de vele

(menselijke) factoren significant lager kunnen uitvallen. In die zin geven veel laboratoriumtests dus een soort 'best case' weer.

### *1.13 Wijzigingen*

Indien een Programma van Eisen tussendoor verandert, kan er niet zonder meer worden uitgegaan van uitkomsten van proeven en haalbaarheidstudies die daarvoor hebben plaatsgevonden. De impact van een wijziging in het Programma van Eisen moet kritisch worden geëvalueerd, waarbij de uitgangspunten voor de gewenste functionaliteit opnieuw systematisch moeten worden afgezet tegen de techniek en de wijze waarop deze moet worden ingezet. Nieuwe functionele eisen rond dezelfde techniek kunnen leiden tot een aanpassing van procedures en processen. Andersom: het gebruik van een andere techniek kan leiden tot het gedwongen aanpassen van het Programma van Eisen. Ook kunnen nieuwe procedures en processen leiden tot het aanpassen van de technische eisen en daarmee tot andere technologiekeuzes. Zo kan het gebeuren dat een project dat eerst als haalbaar werd beschouwd, dat niet meer is na het aanpassen van het Programma van Eisen.

### *1.14 Conclusies*

De uitkomst van een biometrische vergelijking is gebaseerd op een statistische analyse. Omdat altijd de kans bestaat dat het systeem een fout maakt, moet er in voorkomende gevallen een beslissing op basis van menslijke waarneming en beoordeling plaatsvinden. Van belang is dat het stelsel van statistische berekeningen voor identificatie (1:n) en verificatie (1:1) verschillend zijn. Dit heeft zijn weerslag op de te verwachten prestaties en daarmee de eisen die men aan een biometrisch systeem kan stellen. Eisen die voor een 1:1 systeem reëel zijn, kunnen voor een 1:n systeem onhaalbaar zijn. De kengetallen FAR en FRR vertegenwoordigen vaak tegengestelde belangen. Het is daarom van het grootste belang dat bij het opstellen van het Programma van Eisen duidelijk is hoe de relatie tussen de belanghebbenden is en wat het gewicht is van hun inbreng. Als de bestrijding van fraude prioriteit heeft, zal een lage FAR en een grondige registratieprocedure noodzakelijk zijn. Dat kan leiden tot een hoge FRR en een gebruikersonvriendelijk proces, hetgeen voor de

operatie onwenselijk kan zijn. Krijgt de FRR de overhand, dan zal de FAR toenemen en dus de veiligheid afnemen.

De kwaliteit van de geregistreerde biometrische gegevens is van doorslaggevend belang voor de prestaties van het gehele biometrische systeem. De FpVTE van het NIST uit 2003 is een belangrijke bron van informatie over de prestaties van biometrische identificatiesystemen (1:n) en de factoren die deze prestaties beïnvloeden. Echter, het bestaande kwaliteitsbeoordelingssysteem (Nist Fingerprint Image Quality, NFIQ) is op dit moment het belangrijkste kwaliteitstool, maar nog niet voldoende om in een systeem met biometrische apparatuur van meerdere leveranciers uniforme kwaliteit te waarborgen. Een internationale standaard voor de kwaliteit van vingerafdrukken of gezichtsopnamen is in ontwikkeling, maar is de komende jaren nog niet beschikbaar. Dat betekent dat het wisselen van leverancier voorlopig nog tot problemen kan leiden. Maar er is hoop: hoe beter de kwaliteit van de biometrische gegevens, hoe kleiner die problemen zijn.

Duidelijke eisen en een grondig onderhandelingsproces zijn noodzakelijk voor het goed kunnen bepalen van de gewenste drempelwaarden zoals voor de FRR en de FAR. Weloverwogen en goed doordachte drempelwaarden zijn noodzakelijk voor het kunnen evalueren van de prestaties van een biometrisch systeem. Een helder, eenduidig en realistisch Programma van Eisen is een absolute voorwaarde voor het succesvol implementeren en evalueren van een biomterisch systeem, waarbij altijd gekeken wordt in hoeverre het systeem in staat moet zijn om het onderhavige probleem te kunnen oplossen.

## 2. Biometrie: het proces

### *2.1 Biometrie in historisch perspectief*

Om een beter begrip te krijgen van de uitdagingen waar wij voor staan bij het bevolkingsbreed uitrollen van biometrische identificatie, is het belangrijk om inzicht te hebben in het historisch gebruik van biometrie. Terecht zeggen mensen dat biometrie niet nieuw is. We gebruiken het immers al vele tientallen jaren. Wat echter niet altijd wordt erkend is dat het beoogde gebruik zoals bij het biometrische paspoort, weldegelijk nieuw is. Het biometrische paspoort betekent namelijk een verschuiving van het gebruik van biometrie (in dit geval met name de vingerafdruk) van justitiële toepassingen (immigratie, asielprocedures, strafrecht: biometrie voor identificatie) naar publieke toepassingen (documentfraude, verificatie van identiteit voor diensten zoals automatische grenspassage, authenticatie).

De verschillen zijn groot vanwege de volgende verschuivingen.

- Van gesloten naar open doelgroep.
- Van veroordeelden/gearresteerden/verdachten naar onschuldigen.
- Van black list (gedwongen medewerking) naar white list ('vrijwillige' medewerking).
- Van ervaren naar onervaren omgeving.
- Van papier en inkt naar digitaal.
- Van bestaande naar nieuwe infrastructuur.
- Van bestaande naar nieuwe processen.
- Van tien vingers naar twee of vier vingers
- …


*Figuur 4: biometrie met papier en inkt, www.commons.wikimedia.org*

De ontwikkeling *van papier en inkt naar digitaal* heeft een aantal belangrijke gevolgen. Circa vijftien jaar geleden is men bij politie en andere justitiële organisaties begonnen met het digitaliseren van de biometrische databestanden. Dat is begonnen met het inscannen van de ouderwetse vingerafdrukformulieren (zie figuur hierboven) volgens de FBI-standaard. Geleidelijk aan is men digitale vingerafdrukken gaan afnemen, zodat deze direct in de digitale vorm konden worden opgeslagen. Zo is een aantal aspecten drastisch veranderd.

| Vroeger | Nu |
|---|---|
| Uitsluitend lokaal raadpleegbaar. | Raadpleegbaar vanaf 'ieder' werkstation. |
| Er bestond slechts één origineel, kopie was als zodanig herkenbaar. | Origineel op meerdere plaatsen, kopie niet van origineel te onderscheiden. |
| Zoekacties waren tijdrovend en arbeidsintensief (kostte soms enkele dagen). | Zoekacties kunnen snel en efficient (van real time tot enkele uren). |
| Omvang databases beperkt. | Omvang databases praktisch onbeperkt. |
| Uitwisseling door middel van fysieke overhandiging (post). | Uitwisseling door middel van elektronische systemen. |

*Figuur 5: ontwikkeling digitaliseren biometrie, http://www.eubiometricsgroup.eu/*

We zijn bij het gebruik van biometrie gewend aan gesloten doelgroepen. Het betreft dan een beperkt aantal personen (van enkele tienduizenden tot maximaal enkele honderdduizenden), die een specifieke juridische status hebben (bijv. verdachten, gedetineerden, asielzoekers). Dat betekent dat het gebruik van biometrie onder een strikt juridisch en operationeel regime plaatsvindt en op verplichte basis:

- Er is direct contact tussen de te registreren persoon en de overheidsmedewerker.
- De overheidsmedewerker is getraind en gespecialiseerd in het afnemen van de vingerafdrukken, waarbij zelfs fysiek contact is om te zorgen dat de te registreren persoon een goede kwaliteit vingerafdruk produceert.
- In deze situatie van strenge supervisie is het vrijwel uitgesloten dat de te registreren persoon een valse vingerafdruk afgeeft.
- Er worden hoogwaardige vingerprintscanners gebruikt met automatische segmentatie, zodat wordt voorkomen dat foutieve vingers worden geregistreerd.
- De technische infrastructuur is door de jaren heen organisch gegroeid.

Door de jarenlange ervaring met de biometrie is er een beeld van hoe het biometrische systeem in deze omgeving presteert. Onder het bovengenoemde regime zijn de prestaties geoptimaliseerd en weten we wat we van de biometrie kunnen verwachten, zowel wat betreft de veiligheidsaspecten als de nauwkeurigheid. Omdat de vingerafdrukken in dit geval worden gebruikt ter vaststelling van de identiteit is er sprake van identificatie (1:n). Het verifiëren van de identiteit (1:1) aan de hand van de vingerafdrukken is in dit scenario niet gebruikelijk. Het uitgangspunt is dat de vingerafdrukken zekerheid moeten bieden over een identiteit, omdat een bestaande identiteitsclaim hetzij afwezig dan wel onbetrouwbaar is. Het historische gebruik van biometrie kenmerkt zich dus door het gebruik van biometrie (i.c. de vingerafdruk) als identificatiemiddel.

Het beoogde gebruik van de vingerafdrukken zoals omschreven in de Paspoortwet is omvangrijker en is in dit kader nieuw. Onder voorwaarden kan volgens de wet een 1:n zoekactie plaatsvinden op basis van de vingerafdrukken. Dit herkennen we van

het historische gebruik. Het primaire doel is echter het bestrijden van 'look alike fraude'. Daarvoor is er op basis van de Europese verordening EC 2252/2004 een chip in het paspoort geplaatst met als doel het opslaan van onder andere de vingerafdrukken van de houder. Omdat het paspoort de identiteitsclaim voorstelt, heeft de biometrie een verificatiefunctie: het 1:1 controleren of de biometrie in het paspoort overeenkomt met de biometrie van de persoon die aan de hand van dat paspoort een identiteit claimt. Deze processen leggen een grote verantwoordelijkheid bij het registratieproces dat nu plaats moet vinden op honderden locaties door personeel dat geen ervaring heeft met het afnemen van vingerafdrukken. Paragraaf 9.2 gaat in op de wijze hoe de gemeentelijke ambtenaren geïnstrueerd zijn over de techniek en het afnemen van vingerafdrukken. Een ander groot verschil met het historische gebruik is de schaalgrootte: een bevolkingsbrede registratie van vele miljoenen personen ten opzichte van gesloten databases met enkele tienduizenden geregistreerden.

Omdat het beoogde gebruik van de biometrie in het kader van de nieuwe Paspoortwet zowel het historische gebruik betreft als de functie van verificatie van de paspoorthouder (bijv. bij grenspassage), zou tenminste een regime moeten gelden zoals we dat gewend zijn bij justitiële organisaties, als we althans aan dezelfde nauwkeurigheidseisen willen voldoen. Het mes snijdt aan twee kanten: omdat de schaalgrootte een veelvoud is van wat we gewend zijn en daardoor de foutmarges en kansen op fraude groter zullen zijn, en omdat er bij het paspoort sprake is van een basisregister van de gehele bevolking, zouden bepaalde eisen zelfs hoger moeten liggen.

### *2.2 Mis-matchtechniek en verwachting*

Een uitspraak van oud-minister van justitie Korthals uit december 2001 illustreert hoe makkelijk er een mis-match ontstaat tussen de techniek en de resultaten die men ervan verwacht.

*"(...) in antwoord op de vraag van het lid Wijn van Uw kamer [ben ik] niet bereid om van alle Nederlanders vingerafdrukken te nemen in het belang van de*

*opsporing. Dit middel is buitenproportioneel gelet op bijvoorbeeld het aantal aangeboden sporenzaken op jaarbasis, in geheel Nederland ca. 10.000. Voorts is het praktisch onuitvoerbaar omdat alle tien de vingers en eventueel de handpalmen moeten worden afgenomen, wil het zinvol zijn voor de opsporing. Dat vergt een te groot beslag op de capaciteit van de politie. Dit nog afgezien van de administratieve verwerking en controle. In het kader van het nieuwe identiteitsbewijs wordt mogelijk een biometrisch kenmerk opgenomen zoals bijvoorbeeld een vingerafdruk. Daar gaat het er om te bepalen dat de bezitter van het identiteitsbewijs ook daadwerkelijk [de] persoon is die op dat bewijs staat vermeld. Daarvoor is wellicht één vingerafdruk voldoende, dat is echter volstrekt onvoldoende voor de opsporing."*[10]

Uit het bovenstaande citaat spreekt het besef wat er in de praktijk nodig is om een landelijke biometriedatabase succesvol te laten zijn voor opsporingsdoeleinden: er moeten veel meer vingers worden afgenomen (zelfs inclusief een palmprint!) en de minister stelt dat alleen gekwalificeerd personeel dat moet doen (namelijk de politie). Die hebben immers de juiste kennis en ervaring. De minister spreekt hier uit ervaring. Hij weet wat er daadwerkelijk nodig is om het doel van opsporing te bereiken en doet zelfs een principiële uitspraak over proportionaliteit. De partij die voorstaat om een centrale database met de vingerafdrukken van de hele bevolking te gebruiken voor opsporingsdoeleinden, heeft dit besef duidelijk in mindere mate. Tweede Kamerlid Wijn van het CDA hierover:

*"[Het CDA] vindt (…) dat er een meer algemene bereidheid moet worden geconstrueerd voor het afstaan van vingerafdrukken, want dat verhoogt het oplossingspercentage. In de brief van de minister worden daar praktische argumenten tegen ingebracht, zoals het aantal aangeboden sporenzaken, het aantal vingers en de politiecapaciteit, maar geen principiële."*[11]

10 Brief van de minister van Justitie (Benk Korthals) d.d. 10 december 2001, *Kamerstukken II*, 2001-2002, 19637 (Vluchtelingenbeleid), nr. 635, p. 7.

11 Algemeen Overleg met minister Korthals d.d. 13 december 2001, *Kamerstukken II*, 2001-2002, 19637, nr. 642, p. 3-4.

In feite zijn bovenstaande discussies het eerste begin van de onderhandelingen over het Programma van Eisen voor het biometrische paspoort. Dat de twee partijen een verschillende opvatting hebben over nut en haalbaarheid wordt in deze korte citaten direct al duidelijk. De toch vrij principiële argumenten van de minister worden tamelijk eenvoudig van tafel geveegd als zijnde niet principiëel. Wanneer op die punten in een vroeg stadium geen helderheid wordt gecreëerd, kunnen in het verdere proces onduidelijke en soms onrealistische uitgangspunten een hardnekkig leven gaan leiden. Overigens is het riskant om te spreken over 'het construeren van meer algemene bereidheid'. Als bij burgers een tegenzin ontstaat voor het laten van afnemen van biometrische gegevens, zijn er allerlei mogelijkheden om dat te frustreren.

### *2.3 Drivers*

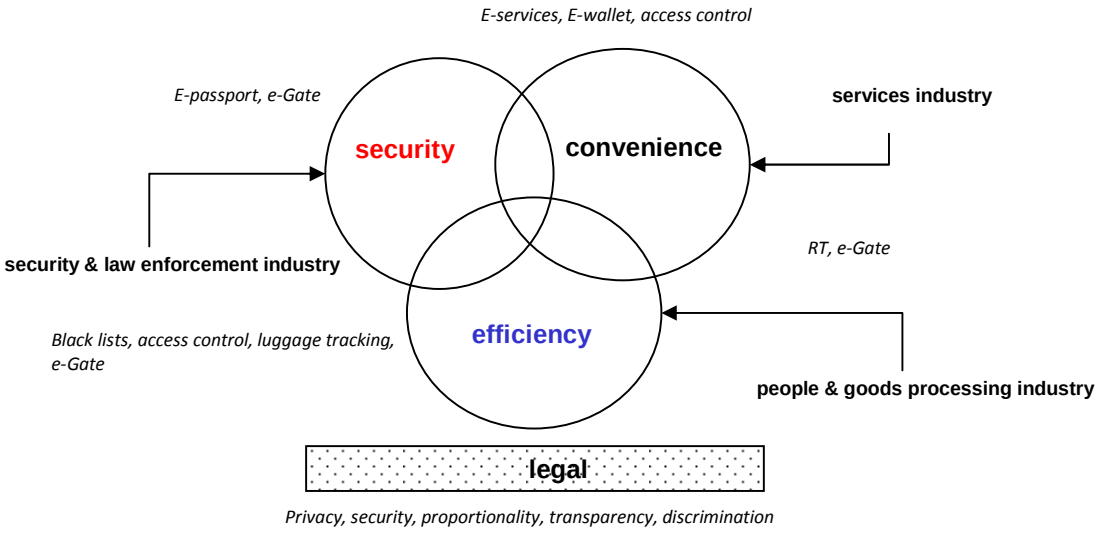
Hiervoor, met name in paragraaf 1.8, is het belang geschetst van een scherp en afgebakend Programma van Eisen. Een PvE moet goed kunnen worden verdedigd door realistische en kwantificeerbare argumenten, zodat het gaandeweg de onderhandelingen en uitvoering in stand kan worden gehouden. Daarvoor is het nodig de primaire *drivers* voor het gebruik van biometrie goed te doorgronden, te benoemen en te handhaven. Over het belang van het stellen van heldere eisen en de juiste *business drivers* zegt Arnout Ruifrok, wetenschappelijk onderzoeker beeldonderzoek en biometrie bij het NFI (Nederland Forensisch Instituut[12]), het volgende.

*"Als men van het begin af aan niet helder heeft wat men nu precies wil doen en wat men wil testen en controleren, dan gaat je hele systeem niet werken. Dan zit je bijvoorbeeld voortdurend je false accept tegen je false reject rate in te sturen. Je moet keuzes maken: waar gebruiken we het voor en hoe pakken we dat het beste aan voor het beste resultaat? Wat men zich niet realiseert is dat verschillende vragen en verschillend gebruik tegenstrijdig kunnen zijn. En als je probeert om beide te optimaliseren, dan gaat dat niet, want je kan ze niet beide optimaliseren. Dat levert ellenlange discussies op waarbij je langs elkaar heen gaat praten. Het*

12 http://www.forensischinstituut.nl.

*inzicht dat het niet allebei tegelijk kan op hetzelfde moment met hetzelfde systeem in dezelfde procedure in dezelfde setting, dat inzicht bereikt men maar moeizaam."*[13]

Het gebruik van biometrie kent verschillende drivers, ofwel redenen waarom biometrie een toegevoegde waarde zou kunnen leveren aan een zeker proces. De drie belangrijkste drivers zijn veilgheid (*security*), gebruikersgemak (*convenience*) en efficiëntie (*efficiency*). De afbeelding hieronder geeft een overzicht.




*Figuur 6: de biometrische business drivers, http://www.eubiometricsgroup.eu/*

Bij biometrietoepassingen is meestal sprake van een mix van de drie drivers; er spelen tegelijkertijd meerdere drivers een rol. Het is van belang om de onderlinge relatie en wisselwerking te begrijpen en om te bepalen welke van de drie drivers dominant is.

Van de drie drivers is veiligheid nog steeds de meest voorkomende. Toegepast in justitiële omgevingen wordt de biometrie gebruikt om delicten op te lossen. Het uiteindelijke doel is om de veiligheid van burgers te beschermen. Ook bij

13 WRR-interview d.d. 18 februari 2010.

toegangscontrole is het de veiligheid die door middel van biometrie moet worden verhoogd: het moet zekerheid verschaffen of autorisatie wordt verleend aan de juiste persoon en niet aan iemand die andermans toegangspasje gebruikt. Zo heeft Schiphol Airport irisherkenning toegevoegd aan bepaalde personeelsdoorgangen. De biometrie is daar een toevoeging op bestaande beveiligingsmiddelen. Het maakt de doorgang niet efficiënter of gebruiksvriendelijker. Integendeel: het proces duurt langer en een personeelslid moet meer handelingen verrichten. De veiligheid staat hier boven convenience en efficiency. De investeringsbeslissing is hier gebaseerd op een risicoanalyse. Dat zijn meestal lastige afwegingen, omdat de kosten en baten rond veiligheidsvraagstukken vaak moeilijk zijn te kwantificeren. Zeker bij een overheid is er een veelheid aan invloeden zoals politieke overtuigingen en intenties, internationale betrekkingen, nationale veiligheid en opvattingen rond veiligheid en privacy. Zeker wanneer een overheid de burgers op basis van een wettelijke verplichting aan een biometriesysteem wil onderwerpen, is het belang des te groter dat er heldere communicatie is ten aanzien van doel, nut, noodzaak, beveiliging en privacy. Want het kan behoorlijk lastig zijn iemand onder normale omstandigheden te dwingen zijn biometrische gegevens af te laten nemen als hij/zij dat niet wil.

Er zijn ook voorbeelden waarbij efficiency de belangrijkste driver is voor een biometrische toepassing. De kern van de toegevoegde waarde zit dan in het geautomatiseerde aspect van de toepassing. In eerste instantie moet zo'n toepassing leiden tot bijvoorbeeld het verminderen van personeel of tot het afhandelen van meer transacties met dezelfde hoeveelheid personeel. Voor dit soort toepassingen is het meestal goed mogelijk om de toegevoegde waarde te kwantificeren, zodat een heldere kosten-batenanalyse ontstaat. Het evalueren ervan kan heel zakelijk: de criteria zijn kostenbesparingen en/of een toename in het aantal transacties per tijdseenheid. Dit zijn vaak systemen waar in korte tijd grote aantallen biometrische datasets moeten worden doorzocht, zoals bijvoorbeeld bij een AFIS. Een ander voorbeeld is het houden van een *watchlist* met gezichtsopnames in combinatie met automatische gezichtsherkenning. Bij grote databases heb je veel mensen nodig om alle gezichten te kunnen herkennen. Mensen kunnen namelijk slechts een gering aantal gezichten onthouden en worden bovendien relatief snel vermoeid, waardoor ze fouten gaan maken. Automatische gezichtsherkenning kan duizenden gezichten opslaan, vertoont

geen vermoeidheidsverschijnselen en is daarom efficiënter dan wanneer dat handmatig moet gebeuren.

Tenslotte kan het verbeteren van het gebruikersgemak een reden tot invoering van biometrie zijn. Denk daarbij vooral aan commerciële toepassingen, zoals het vervangen van een pincode of smartcard voor het verkrijgen van toegang tot diensten. Biometrisch betalen is daarvan een voorbeeld. Daar staat de dienstverlening naar de gebruiker centraal. De toegevoegde waarde moet evident zijn, omdat de gebruiker het systeem vrijwillig gaat gebruiken en er soms een zeker bedrag voor over moet hebben. Meestal speelt veiligheid in dit soort toepassingen wel een rol, maar meer als een randvoorwaarde dan een primair doel. Het commerciële karakter van dit soort toepassingen zorgt voor een heel ander soort afwegingen. Zo zal de proportionaliteit vanuit het oogpunt van privacy niet vanuit een maatschappelijke noodzaak worden bekeken. Omdat de gebruiker vrijwillig deelneemt, kan hij/zij de service altijd opzeggen bij gebrek aan vertrouwen in de integriteit van het systeem. Een goed geregelde privacy vertegenwoordigt voor de aanbieder zodoende een commercieel belang.

Op de volgende pagina's wordt ogenschijnlijk een en dezelfde toepassing beschreven, namelijk grenspassage op een luchthaven. Nadere analyse laat zien dat het om drie verschillende business cases gaat, met verschillende belangen en doelstellingen.

***Voorbeeld 1: reguliere grenscontrole***

*De oorspronkelijke bedoeling van het biometrische paspoort is het voorkomen van 'look alike fraude' bij grenscontrole. Het is echter nog maar de vraag of de frequentie van 'look alike fraude' de inzet van een biometrisch paspoort kan dragen. De primaire driver bij reguliere grenscontrole is dus security, hoewel men zich wel zorgen maakt over de tijd die een biometrische controle in beslag neemt. Dat is niet zozeer vanwege de reiziger, maar meer voor de efficiency van het proces. De toegevoegde waarde voor de gebruiker (i.e. de marechaussee) is het kunnen gebruiken van een extra middel tegen 'look alike fraude'.*

*Figuur 7: paspoortcontrole op Schiphol Airport*

***Voorbeeld 2: de e-Gate***

*De constant toenemende stroom van passagiers op luchthavens zorgt voor steeds langere rijen. Terwijl het aantrekken van meer personeel vaak geen optie is vanwege de kosten, moeten deze grote aantallen passagiers toch op een veilige en prettige wijze door het luchthavenproces worden geleid. Als dat niet gebeurt, ontstaan er chaotische situaties en ontevreden reizigers. Dat gaat ten koste van zowel de veiligheid als de kwaliteit van de reiservaring. Beide vormen een bedreiging voor de business van een luchthaven of airline. Bij intensieve en complexe passagiersbewegingen kan biometrie zorgen voor een hogere efficiency, terwijl tegelijkertijd het beveiligingsniveau en het gebruikersgemak worden verbeterd. De belangrijkste driver in deze toepassing is efficiency, omdat de toegevoegde waarde voor de gebruiker (i.e. de luchthaven) op efficientere wijze het grenspassageproces kan faciliteren.*

***vandaag*** ***morgen***

*Figuur 8 en 9: poorten voor automatisch grenscontrole, gebaseerd op het e-paspoort en biometrie; standaards en interoperabiliteit zijn cruciaal; rechts: e-Gates in portugal (RAPID), http://www.rapid.sef.pt/*

***Voorbeeld 3: Privium***

*Privium op Schiphol Airport is een op service gebaseerde automatische grenspassage. Naast een snelle passage door de Privium Gate biedt het prgramma parkeerfaciliteiten en een luxe lounch. Het programma richt zich op de zakelijke reiziger en kost € 125,- per jaar. Het systeem gebruikt de irisscan als operationele biometrie en een speciale smartcard, waarop, naast de lidmaatschaps- en persoonsgegevens, ook de twee iriscodes staan opgeslagen (links en rechts). De kaart wordt onder direct toezicht van de marechaussee uitgegeven. De primaire business driver is hier convenience, omdat de toegevoegde waarde voor de gebruiker berust op service en gebruikersgemak. Het wordt dan ook als een commerciële dienst op de markt aangeboden.*


*Figuur 10: de automatische poort is transparant en gebruikersvriendelijk*

*Figuur 11: de luxe Privium Club Lounge (Members Only)*

De bovenstaande voorbeelden geven aan hoe onderscheidend de rol van biometrie kan zijn in de context van een enkele toepassing, in dit geval grenscontrole. De verschillen in de business case maken dat processen en procedures anders worden ingericht, andere technologiekeuzes worden gemaakt, andere succesfactoren worden gedefinieerd, een andere proportionaliteitsafweging wordt gemaakt en zelfs dat er verschillende financieringstructuren worden gekozen. Dat laatste is zeker niet onbelangrijk, want meestal geldt: wie betaalt, bepaalt.

Het wordt ingewikkeld wanneer de drie business drivers een gelijke mate van belang hebben in het creëren van een succesvolle toepassing. De eisen van de belanghebbenden hoeven niet altijd met elkaar overeen te komen. Soms is er zelfs sprake van tegenstrijdigheid. Zowel de eisen als de succescriteria zijn dan verschillend. Er volgen dan onderhandelingen waarvan een goede uitkomst niet altijd is verzekerd. Het zal niet de eerste keer zijn dat een biometrieproject strandt, omdat de belanghebbenden niet op één lijn zitten. Als je daar te laat achter komt, kunnen de gevolgen catastrofaal zijn. Zo is bij de opening van Terminal 5 van London Heathrow op het laatste moment een streep gehaald door de biometrische boarding. Daarbij zou door middel van een biometrie aan de gate worden gecontroleerd of alle juiste personen in het vliegtuig zitten. Hoewel de vingerafdrukken uitsluitend voor dat doel gebruikt zouden worden, werden deze data tot 48 uur na het opstijgen van het vliegtuig bewaard. Op het allerlaatste moment is deze toepassing onder druk van een heftige privacydiscussie geschrapt, omdat niet duidelijk was waarom de data niet direct na het boarden zouden worden gewist. Het kan vervolgens lang duren voordat een project weer een tweede kans krijgt.[14]

In situaties van meerdere belangen is het sluiten van compromissen soms een riskante zaak, omdat dit al snel kan leiden tot een onduidelijk Programma van Eisen en – daarmee samenhangend – vage succescriteria. Een evaluatie achteraf van de kosten-batenanalyse van het systeem kan dan lastig worden. Dergelijke projecten stranden regelmatig nog voordat zij het daglicht zien, bijvoorbeeld omdat men het 'te duur' vindt. Zonder kwantitatieve argumenten is daar weinig tegen in te brengen, want 'te duur' is een perceptie. Het stopzetten van het biometrische paspoort in Engeland onder de nieuwe regering-Cameron vindt onder andere daarin zijn oorzaak: in tijden van bezuinigingen worden eerst de projecten geschrapt waarvan de kosten significant zijn en de toegvoegde waarde onduidelijk is.

Om mislukking te voorkomen is het een eerste voorwaarde dat er een helder Programma van Eisen is. Daarin moet de functionaliteit van de biometrie duidelijk zijn beschreven en tot in detail uitgewerkt in processen en procedures. Maar ook de

14 *Telegraph Online* (UK), 28 maart 2008, Heathrow Terminal 5 fingerprint plans 'illegal".

functionele beperkingen die aan het systeem worden opgelegd (de zogenaamde finaliteit) moet worden vastgelegd. Het duidelijk benoemen van de drivers is daarbij onmisbaar. Bij projecten waar nieuwe technologie het centrum vormt van de functionaliteit van de toepassing kan dit een grote uitdaging zijn. Om de toegvoegde waarde van de biometrie te bepalen is het altijd nuttig zich de vraag te stellen: wat is het alternatief en wat gebeurt er als ik niets doe. Echter, nieuwe tot de verbeelding sprekende technologie heeft vaak het effect dat mensen graag willen geloven dat er als het ware een nieuwe wereld mee geschapen kan worden, terwijl de risico's dan nog niet goed worden begrepen.

Dat effect wordt nog eens groter wanneer 'Hollywood' en andere media nieuwe technologie als feilloos en/of zaligmakend afschilderen. Dat geldt ook voor biometrie met films als Minority Report, Charlie's Angels en CSI. De prestaties van de in deze films getoonde biometrische apparatuur spreken zeer tot de verbeelding, maar zijn niet op alle punten realistisch. Maar de beeldvorming die hieruit ontstaat heeft een grote invloed en raakt ook bewindslieden, beleidsmakers en politici. Door het gebrek aan echte ervaring met biometrie krijgt dit soort beeldvorming makkelijk de overhand, omdat de techniek nog niet voldoende aan de praktijk is getoetst. Experts moeten er aan te pas komen om dit soort beeldvorming op basis van goede argumenten te kunnen relativeren. Maar dan moeten zij wel gehoord worden. Ook voor biometrie geldt dat de fascinatie voor de techniek regelmatig leidt tot onrealistische opvattingen over de toepassingsmogelijkheden. Uiteindelijk zal de praktijk dit beeld corrigeren, maar soms kan daar veel tijd (en geld) overheen gaan.

## 3. Conclusies Deel I: Techniek en proces

Het ontwerpen van grootschalige biometrische toepassingen is complexer dan men in eerste instantie zal denken. Zeker wanneer er verschillende functionele eisen worden gecombineerd in één Programma van Eisen neemt de complexiteit en daarmee de kans op compromissen, lagere prestaties en hogere kosten toe. Het verschuiven van een verificatiefunctie naar een identificatiefunctie betekent een ingrijpende verandering in de architectuur. Dat betekent dat de eisen en de haalbaarheid ervan in principe volledig moeten worden herzien.

Zonder enige twijfel is de belangrijkste voorwaarde voor een goed functionerend biometrisch systeem de kwaliteit en integriteit van de opgenomen biometrische informatie (*images*). Dat geldt in grote mate voor de *enrolment* (zeker bij 1:n zoekfuncties), maar ook bij verificatie. Zeker bij onzekerheid over te verwachten prestaties is het streven naar een optimale kwaliteit van de biometrische informatie een absoluut eerste vereiste. Compromissen op dat punt (bijv. goedkopere scanners, beperkte training van baliemedewerkers etc.) betekenen al snel een significante verslechtering van de prestaties van het systeem als geheel met als gevolg lagere betrouwbaarheid, meer fouten, trage respons, hogere kosten etc.

Een ander fenomeen waarmee rekening gehouden moet worden betreft manipulatie. Vingerafdrukken kunnen op heel subtiele wijze worden nagemaakt, zonder dat het biometrische systeem dat opmerkt. Het vergt aandacht en expertise van de baliemedewerkers om zulke gevallen te herkennen. Voor een systeem dat dubbele identiteiten moet kunnen detecteren aan de hand van biometrie is dat een belangrijk punt van aandacht.

Naast kwaliteit en het gevaar van manipulatie vormen de verschillende drivers achter het gebruik van biometrie, en de specifieke voorwaarden die de verschillende drivers met zich meebrengen voor het goed functioneren van een biometrisch systeem punt van aandacht. Het op één hoop gooien van verschillende toepassingen, omdat zij alle gebruikmaken van biometrie is hierdoor riskant, omdat de onderliggende drivers en

doelstellingen – en daarmee de functionele en technische uitvoeringsvorm van de toepassingen – verschillend zijn.

Binnen justitiële kringen, waar men uitgebreide ervaring heeft met biometrie, worden andere (met name hogere) eisen gesteld aan techniek en processen dan niet-ervaringsdeskundigen vermoeden. Dit werkt een mis-match tussen de techniek en het doel dat het moet dienen in de hand. Het extrapolleren van de binnen Justitie geldende eisen ten aanzien van het gebruik van biometrie naar een bevolkingsbrede uitrol, levert naar inschatting van de toenmalige minister van Justitie een disproportioneel systeem op.

Tot slot moet nog gewezen worden op de perceptie van wat er allemaal mogelijk zou zijn met biometrie. Deze perceptie wordt voor een niet te onderschatten deel beïnvloed door wat men ziet in films en op televisie, zoals *Minority Report*, *Chrarlie's Angels* en *CSI*. In zulke gevallen wordt er veelal een te optimistisch en te simplistisch beeld geschets van het gebruik van biometrie. Dit leidt tot een onrealistisch beeld bij brede groepen van de bevolking.

# DEEL II Industrie, markt en standaardisatie

# 4. Industrie en markt

## *4.1 Inleiding*

Nu we inzicht hebben in de belangrijkste technische aspecten van biometrie, willen we weten hoe het landschap van de biometrische markt eruitziet. In het volgende deel wordt gekeken naar het historische gebruik van biometrie en welke invloed dit heeft op de structuur van de huidige markt. Er zal worden uitgelegd hoe het kan dat een relatief oude markt toch nieuw kan zijn. Verder komen standaardisatie en testen aan de orde, maar ook de slechte balans tussen de marktleiders en nieuwkomers in de markt voor biometrieproducten en -diensten. De richtlijn van de ICAO, Doc9309, heeft rond 2003 de acute noodzaak gecreëerd voor het ontwikkelen van talloze internationale standaards. Het gebrek aan standaardisatie heeft geleid tot een markt waarbij de producten van leveranciers niet uitwisselbaar zijn en waarvan de prestaties onderling niet goed vergeleken kunnen worden. Deel II zal het belang aantonen van het onafhankelijk laten testen van biometrische componenten en systemen. Daarvoor zullen twee van de belangrijkste biometrische projecten ter wereld op dit moment, te weten het Biometric Matching System van de Europese Commissie en het Indian Unique Identity Project, worden besproken. Omdat het belang van een goede enrolment groot is, worden de resultaten van het project BioDev besproken en de wijze waarop Duitsland mede op basis van die uitkomsten de kwaliteit van de enrolment heeft verbeterd. BioDev is een testprogramma dat is ontwikkeld om het biometrische aanvraagproces voor een Europees visum op consulaire posten te analyseren en te optimaliseren.[15] Tenslotte wordt het belang aangegeven van het uitvoeren van grondige end-to-end tests, waarbij alle componenten van een biometrisch systeem worden geëvalueerd, inclusief processen, procedures en operationale omstandigheden, met wederom extra aandacht voor de kwaliteit en integriteit van het registratieproces.

In de volgende paragrafen kijken we waar in het complexe geheel van de markt er voor biometrie kansen liggen voor de industrie en hoe daarop wordt ingespeeld.

15 Voor meer informatie zie: http://www.findbiometrics.com/articles/i/5081/ en http://www.findbiometrics.com/articles/i/5081/.

### *4.2 Kansen AFIS-markt*

Nationaal en internationaal is met name veiligheid de belangrijkste drijfveer voor het in gebruik nemen van biometrie waarbij de overheid verreweg de grootste afnemer is. Of dat altijd op een goed uitgewerkte business case is gebaseerd valt nog te bezien. Het gebruik van biometrie in nationale identiteitssystemen zoals bevolkingsadministraties heeft zijn toegevoegde waarde nog niet bewezen. Vanuit justitiële hoek kan men een realistischer kijk op het gebruik van biometrie verwachten. Daar heeft men veel ervaring met biometrie en is sprake van een uitgebreide *installed base* (i.e. de de verzameling van de reeds geïnstalleerde systemen). Die bestaande systemen moeten worden onderhouden en uitgebreid. Dat laatste heeft te maken met de groei van de databases (bevolking groeit, criminaliteit groeit) en de groeiende noodzaak voor het Europees en internationaal uitwisselen van gegevens van immigranten, asielzoekers en (zware) criminelen. We hebben het hier dan vrijwel uitsluitend over AFIS-systemen voor nationale markten.

De internationale markt voor AFIS laat het beeld zien van nationale verkaveling. Slechts een beperkte groep leveranciers levert aan dit segment. Het beeld is dat elk land zijn eigen hofleverancier daarvoor heeft, waardoor de markt min of meer nationaal is verkaveld. Omdat het aantal landen zich niet uitbreidt, is er sprake van een verdringingsmarkt. De kansen in dit segment zitten met name in opschaling van de systemen en het toevoegen van functionaliteit met betrekking tot uitwisseling van data en toegang tot de systemen. Uiteraard worden met deze opschaling zaken als prestaties en betrouwbaarheid (en daarmee samenhangend kwaliteit, snelheid en efficiency) steeds belangrijker. Innovatie binnen dit segment vindt dan ook vooral op die punten plaats. Zoals in paragraaf 4.5 over *Gevestigde orde vs nieuwkomers* zal worden beschreven, zijn in dit segment de grote industriële spelers dominant.

De ontwikkeling die de laatste jaren zichtbaar wordt is dat naast de bekende AFIS-leveranciers (zoals Morpho (voorheen Sagem), Cogent, NEC (en vroeger ook Motorola) ook gevestigde systeemintegratoren deze markt proberen te betreden. Voorbeelden zijn Accenture, IBM, Logica, ATOS Origin etc. De reden is dat vanwege de schaalvergrotingen en het toenemende gehalte aan ICT de component voor systeemintegratie steeds groter wordt en de biometriecomponent relatief kleiner. De

belangrijkste omzet wordt gegenereerd door software (licenties voor databases en algoritmes), systeemintegratie en onderhoud. Voor het betreden van de markt hanteren systeemintegratoren verschillende strategieën.

- Zij werken samen als prime-contractor of als sub-contractor met een van de grote biometriebedrijven; zij halen daarmee de kennis en technologie in huis, alsmede belangrijke contacten met bepaalde overheden, inclusief de reeds geïnstalleerde systemen.
- Zij ontwikkelen hun eigen AFIS door kerntechnologie te kopen bij een (relatief) klein biometriebedrijf (soms zelfs als een acquisitie) en gebruiken hun eigen contacten om als prime contractor systemen aan overheden te leveren.

### *4.3 Het biometrische paspoort als marktsegment*

Het biometrische paspoort is het volgende marktsegment dat grote kansen voor de industrie creëert. Het gaat daarbij wederom om nationale systemen, maar ditmaal met een grotere component voor hardware. Er zijn immers vele plaatsen waar de biometrie geregistreerd moet worden (in elk geval alle gemeentehuizen en consulaire posten) en er zal nog steeds een document moeten worden geproduceerd. Ook zal voor de controle infrastructuur in de nabije toekomst veel hardware geleverd moeten worden voor grenscontroles op land, zee- en luchthavens. Dit illustreert meteen twee kanten van de paspoortmarkt: die van de uitgevende instanties en die van de controlerende instanties. Op dit moment is alleen nog de markt van uitgevende instanties actief. Maar op beurzen en conferenties is zichtbaar dat de industrie al proactief inspeelt op de controlerende instanties door veel ontwikkeling te steken in bijvoorbeeld mobiele biometrische leesapparatuur. Net zoals bij de uitgevende instanties is het voordeel ook van deze markt dat de overheid met zekerheid grote investeringen zal gaan doen. De vraag is alleen wanneer. Het nadeel is namelijk dat de besluitvormingsprocessen lang duren en afhankelijk zijn van politieke besluitvorming en internationale ontwikkelingen. Voor kleine bedrijven levert dat grote problemen op, zeker als die daarbij ook nog jong zijn en nog niet over de juiste contacten en referenties beschikken.

Onder invloed van de centrale personalisatie, de contactloze chip met bijbehorende PKI en de toevoeging van biometrie is de paspoortmarkt zich sinds ca. 2000 steeds meer aan het ontwikkelen als segment van de ICT-industrie. Daar waar het paspoort vroeger bijna uitsluitend een grafisch product was, is de ICT-component dermate uitgebreid geworden dat ook het voormalige Enschedé/SDU (tegenwoordig Sagem[1] Identification) haar contract met de overheid alleen invulling kon geven met een systeemintegrator als sub-contractor voor het ICT-gedeelte. In Slovenië was HP zelfs de prime-contractor. Hoewel de fysieke locatie van de paspoortleverancier vanuit beveiligingsoogpunt nog steeds bij voorkeur in het land zelf is, zie je dat bepaalde landen besluiten om hun paspoorten elders te laten maken. Ook zijn er paspoortleveranciers die in een ander land productiecapaciteit naar eigen model opzetten om de lokale overheid van identiteitsdocumenten te voorzien.

Met de komst van de centrale personalisatie is de relatie tussen de overheid en de leverancier enigszins veranderd. Waar eerst alleen het transport tussen de leverancier en de klant stond, is dat nu een complete ICT-infrastructuur plus een besloten glasvezelverbinding naar alle gemeentehuizen. De persoonlijke gegevens van alle burgers worden nu binnen de muren van de leverancier verwerkt. Vervoer en opslag van blanco paspoorten was altijd een hachelijke zaak, omdat fraude met blanco paspoorten vrij eenvoudig en evenzo populair was. Dat kan nu niet meer. Er verlaten nu uitsluitend gepersonaliseerde paspoorten de poorten van de leverancier, waardoor het versturen ervan via beveiligde transporten iets minder omslachtig is. Paspoorten worden ook gewoon per post verstuurd. In theorie is de overheid nu dus beter in staat om vrij te kiezen voor een paspoortleverancier. Ook vanuit de mededingingswet en het Europese aanbestedingsbeleid zou dat moeten. In de praktijk gaat dat echter iets anders. Overheden hebben toch graag direct contact met hun leverancier en willen de mensen die er werken kennen. Het gaat om de staatsveiligheid en het vertrouwen in het nationale administratieve systeem, dus zomaar overstappen naar een buitenlandse leverancier (waarbij de paspoorten niet meer in eigen land worden geproduceerd en gepersonaliseerd) is geen kleine stap. De meeste landen houden de voorkeur om het gehele proces op eigen bodem te houden. Relaties tussen vertegenwoordigers van overheid en leveranciers bestaan soms al vele jaren en kunnen met elkaar ‘lezen en schrijven’.

Leveranciers van biometrische paspoorten laten als antwoord op deze veranderingen verschillende strategieën zien.

- Een van oudsher drukker van paspoorten breidt zijn capaciteit uit naar andere landen. Het drukwerk staat centraal. In het land waar een werkmaatschappij is gevestigd zorgt een lokale partij als prime-contractor voor de integratie.
- Historische paspoortfabrikanten breiden hun competenties uit met ICT-kennis en producten, zoals netwerken, PKI en kiosken. Daarmee worden zij als prime-contractor een end-to-end leverancier van een geheel paspoortsysteem.
- Een klassiek biometriebedrijf koopt competenties aan voor het kunnen leveren van ID-managementsystemen en neemt een paspoortleverancier aan als sub-contractor. Voorbeeld is L1, dat de ID-managementdivisie van Digimarc kocht voor het leveren van aanvraag- en uitgiftesystemen voor het Amerikaanse rijbewijs. Het drukken lieten ze aan een andere partij over. Morpho gaat nog een stap verder: dit Franse bedrijf koopt Enschedé/SDU, zodat zij nu een end-to-end paspoortsysteem kunnen leveren, dus inclusief het drukwerk.

Wanneer overheden besluiten om de biometrische gegevens van burgers ook centraal op te slaan en toegankelijke te maken voor bepaalde functionaliteiten, ontstaan er nieuwe kansen voor de in de vorige paragraaf beschreven leveranciers van AFIS-systemen. Zij hebben immers al jaren ervaring met grote vingerafdrukdatabases en bovendien zijn de contacten met de overheid al aanwezig. Sommige leveranciers spreken al van een 'Civil AFIS'.

In dat landschap neemt Morpho, waar ook de biometriedivisie onder valt, een bijzondere positie in. Met de acquisitie van SDU Identification is Morpho in staat om te kunnen leveren op elke positie van de waardeketen in het paspoortaanvraag, productie- en uitgifteproces. Ooit begonnen als de leverancier van vingerafdruksensoren en -algoritmes is het bedrijf via acquisities en eigen ontwikkeling uitgebreid tot een all-inclusive identiteitsmanagementbedrijf. Het levert naast de biometrie (waarmee zij in de top drie van de wereld behoren) ook

smartcards en middleware voor een enorme hoeveelheid verschillende toepassingen. Tegenwoordig is het bedrijf in staat een volledig paspoortaanvraag- en -uitgiftesysteem te leveren, inclusief de integratie van het ICT-gedeelte en de biometrische database. Een grote concurrent, het Amerikaanse biometrieconglomeraat L1 Identity Solutions, is onlangs ook gekocht door Morpho, nadat een paar jaar geleden de biometriedivisie van Motorola al naar Morpho was gegaan.
Een andere wereldspeler in de AFIS-markt, Cogent, is onlangs verkocht aan 3M, een bedrijf dat actief is in de productie van identiteitsproducten zoals paspoortscanners en complete identiteitssystemen. De reden van de overname door 3M is dat zij via Cogent toegang krijgen tot justitiële overheidsorganisaties.

Als het gaat om de biometrische controleapparatuur voor grensmanagement zien we naast de klassieke biometriebedrijven en systeemintegratoren ook bedrijven hun intrede doen uit de defensie-industrie, zoals EADS, Thales, Lockhead Martin en wederom Morpho. Zij kunnen hun bestaande klanten voorzien van extra diensten door hun controleapparatuur te voorzien van biometrische functionaliteit.

### *4.4 Nationale verkaveling van de internationale biometriemarkt*

Het hiervoor beschreven historische gebruik van biometrie heeft geleid tot een nationale vraag naar biometrische producten in met name de justitiële sector, maar met de komst van het biometrische paspoort inmiddels ook binnen andere delen van de overheid. De justitiële vingerafdruksystemen (gebruikt voor o.a. immigratie, asielzoekersprocedures en criminaliteit) zijn dan ook nationale systemen, die slechts op basis van laterale (zoals het Schengen Informatie Systeem) en/of bilaterale verdragen (zoals het meer recente Treaty of Prüm) data van criminelen en asielzoekers uitwisselen. Deze groepen vormen een gesloten groep individuen met een aparte juridische status. Bij aanbestedingen door overheden van dit soort nationale vingerafdruksystemen was interoperabiliteit geen primaire eis. Door een gebrek aan standaards zat een overheid dan al snel vast aan één specifieke leverancier. Hoewel de standaards aanzienlijk zijn verbeterd, domineert dit beeld tot op de dag van vandaag. Een belangrijk gevolg is dat 1) de industrie weinig stimulans

heeft om echte interoperabiliteit te creëren en 2) een overheid meestal voor langere tijd vastzit aan een bepaalde leverancier.

Ondanks de leveranciersafhankelijkheid op nationaal niveau waren de problemen op het punt van internationale uitwisseling van data hanteerbaar.

- De processen, procedures, apparatuur en personele vaardigheden zijn zodanig ingericht dat bij de registratie een optimale kwaliteit van de biometrische informatie wordt verkregen (hoe hoger de kwaliteit, hoe beter de interoperabiliteit tussen leveranciers).
- Er worden tien vingers gebruikt om de kans op een match te vergroten, ook wanneer door gebrek aan interoperabiliteit er kwaliteitsverlies is bij uitwisseling van gegevens aan andere systemen.
- Justitiële diensten houden een back-up database van de images, zodat de gehele database kan worden overgezet naar de specifieke software van de nieuwe leverancier. Dit is op de schaal van een gehele bevolking uiteraard een nogal omslachtige en kostbare operatie.

Het voorgaande illustreert dat de nationale verkaveling van de biometriemarkt, in combinatie met een nog niet goed functionerend systeem rond internationale standaarden, vergaande gevolgen heeft voor de keuzevrijheid voor technologie en leveranciers, de inrichting van de operationele processen en de benodigde vaardigheden van medewerkers.

Een ander gevolg van de nationale verkaveling van de internationale biometrie-industrie is dat de innovatie grotendeels in handen is van de grote biometriebedrijven. Vanwege een aantal overnames zijn dat er tegenwoordig niet veel meer dan drie. Deze grote bedrijven, die vanwege hun vertrouwelijke relatie met hun overheidsklanten en de beperkte uitwisselbaarheid van hun producten niet staan te wachten op nieuwkomers in de markt, hebben vanuit het handhaven van hun marktpositie geen voordeel bij het verbeteren van de interoperabiliteit. En omdat innovatie veel geld kost en nieuwkomers op de biometriemarkt niet snel grote overheidsprojecten krijgen toebedeeld, blijven strategische vernieuwingen op

technisch vlak vaak liggen. De marktleiders innoveren wel, maar met name binnen de scope van hun eigen technologie.

Verder laat de waardeketen van de biometrie industrie de volgende typen bedrijven zien.

- Producenten van kerntechnologie ('biometric vendors', dit zijn er wereldwijd inmiddels een paar honderd).
- Leveranciers van middleware.
- Solution providers.
- Systeemintegratoren.
- Toepassers/afnemers.
- Eindgebruikers.

Dit lijstje lijkt overzichtelijker dan het in de praktijk is: er zijn vendors die ook systeemintegratie doen (bijv. Morpho), en systeemintegratoren die – hetzij door eigen ontwikkeling, hetzij door partnerships of acquisities – ook eigen technologie leveren (bijv. IBM, Accenture). Dat geldt ook voor middleware providers: die ontwikkelen vaak solutions of treden op als systeemintegrator (bijv. DAON). Vaak zijn deze wel onafhankelijk van leveranciers (hun middleware overbrugt de verschillen), hetgeen hun meerwaarde in de markt bepaalt. Bovendien is biometrie in hun visie slechts een onderdeel van de identiteitsmanagementketen, waardoor zij vaak in staat zijn om biometrische functionaliteiten beter in het geheel te integreren dan producenten van kerntechnologie. Maar ook producenten van kerntechnologie ontwikkelen vaak gehele applicaties (bijv. een toegangscontrolesysteem). Dat is nodig, omdat de waardeketen nog niet homogeen is. Leveranciers van kerntechnologie hebben moeite om hun producten aan de volgende ketenspeler te verkoper, omdat de vraag van de klant nog niet zo sterk is. De leverancier van kerntechnologie wordt dan als het ware gedwongen om toepassingen die gebaseerd zijn op zijn technologie over de ketenpartners heen direct aan de afnemers te verkopen.

Zo gering als het aantal marktleiders is, zo groot is het aantal kleine tot middelgrote biometriebedrijven. Die bedienen verschillende marktsegmenten, zoals

toegangscontrole, logical access, surveillance en financiële diensten (bijv. biometrische ATM's). Op www.findbiometrics.com is een aardig overzicht van de biometriebedrijven wereldwijd te zien.

Nederland heeft geen biometrieindustrie van betekenis. Er worden hier nauwelijks biometrische kernproducten gemaakt, zoals vingerafdrukalgoritmen, matching algoritmen of sensoren. Hiervoor zijn we dus afhankelijk van het buitenland.

### *4.5 Gevestigde orde vs nieuwkomers*

Zoals in de vorige paragrafen is beschreven, wordt de biometriemarkt gedomineerd door enkele bedrijven die de gevestigde orde vormen. Na enkele overnames zijn dat er op dit moment nog maar drie: Morpho, 3M en NEC, die dan ook over een internationaal netwerk beschikken. Weliswaar heeft de markt zich uitgebreid van justitieel gebruik naar grootschalige bevolkingsadministraties, maar het zijn nog steeds dezelfde bedrijven die het best gepositoneerd zijn om contracten gegund te krijgen. Naast de grote leveranciers bestaat er een veelheid van kleine producenten van biometrische kerntechnologie, met name innovatieve software, nieuwe modaliteiten en slimme kleinschalige toepassingen. Deze kleinere en meestal jonge bedrijven komen niet snel in aanmerking voor grote projecten, omdat ze te klein zijn voor de risico's en aansprakelijkheden van grote contracten en omdat ze grote referenties missen. Daarbij komt dat de bestaande leveranciers veelal hechte relaties hebben met nationale overheden. Het gaat daar om zaken als de staatsveiligheid en daarbij behoren vertrouwelijke en niet voortdurend veranderende relaties.

Kleinere bedrijven hebben ook meer moeite om deel te nemen aan grote Europese projecten. Die nemen over het algemeen relatief veel overhead met zich mee en worden vrijwel nooit 100% gefinancierd. Dat is moeilijk op te brengen, omdat al hun tijd en geld gestoken moet worden in het ontwikkelen van hun producten en het op peil houden van hun financiering. Ook het veroveren van een plek op de markt vraagt veel van hun schaarse middelen. Het gevolg is dat de kleinere bedrijven, die overigens vaak bijzonder innovatief zijn, moeilijk kunnen profiteren van de huidige marktvraag die met name vanuit de overheid komt. Het effect daarvan is tweeledig.

- Nieuwkomers op de biometrie markt moeten zich gedwongen richten op nieuwe en vaak moeilijk bereikbare marktsegmenten.
- De overheden kunnen niet profiteren van de innovatie van kleine, maar vaak slimme biometriebedrijven.

De grote bedrijven richten zich voornamelijk op het in stand houden van hun bestaande markten en op de nieuwe markten die daar dicht tegenaan liggen, zoals de nationale paspoortprojecten. Zij hebben in deze markten een grote historische 'installed base'. Innovatie is daar niet de prioriteit, maar veel meer het garanderen en uitbreiden van de bestaande functionaliteit. Daarnaast bestaat veel van hun business uit het interoperabel maken en opschalen van de nationale systemen. Kleine nieuwkomers komen daar slechts zelden aan te pas. Dit geheel zorgt ervoor dat in het algemeen de innovatie binnen de biometrie industrie maar moeizaam verloopt.

## 5. Standaardisatie

### *5.1 State of the Art: de ICAO Richtlijn en de Europese doorvoering daarvan*

De standaardisatie van de internationale biometriemarkt is pas echt goed begonnen nadat de ICAO (International Civil Aviation Organization) in 2003 met een wereldwijde richtlijn kwam voor het gebruik van biometrie voor het paspoort (ref. Doc 9303 Machine Readable Travel Documents). De gebeurtenissen van '11 september' hebben dat proces zeker versneld. Deze nieuwe richtlijn schrijft de vingerafdruk, gelaatsscan en de irisscan voor als de technologieën die in de paspoorten opgeslagen moeten gaan worden ter verificatie van de identiteit en ter controle van de authenticiteit van het paspoort. In 2006 is de laatste herziene versie verschenen.[16]

Sinds een aantal jaren heeft de EU gebruik kunnen maken van de resultaten van het werk van de ICAO (o.a. Doc 9303) en heeft haar eisen dan ook daarop gebaseerd. Inmiddels zijn op basis daarvan de volgende Europese standaards ontwikkeld.

16 www2.icao.int/EN/MRTD/Pages/Downloads.aspx.

- Reg (EC) 1683/1995 laying down a uniform format for visas.
- Reg 1030/2002 laying down a uniform format for residence permit for 3rd country nationals.
- Reg 333/2002 on a uniform format for forms for affixing the visa issued by Member States to persons holding travel documents not recognized by Member States drawing up the form.
- Treaty of Prüm, a bilateral treaty between Member States to exchange data (incl. fingerprints) in the framework of police cooperation.

Als doorvoering van Doc9309 heeft de Europese Raad de Richtlijn (EC) No 2252/2004 d.d. 13 december 2004 met betrekking tot standaarden voor beveiligingskenmerken en het opnemen van biometrische gegevens in paspoorten en reisdocumenten aangenomen. Deze richtlijn levert de wettelijke grondslag voor de lidstaten tot het invoeren van een uniform Europees paspoort. Het heeft geleid tot het landelijk uitrollen van vingerafdruksystemen met als doel opslag daarvan in de paspoort chip. Over het doel zegt (EC) No 2252/2004 het volgende.

*"Biometrische gegevens worden verzameld en opgeslagen in het opslagmedium voor paspoorten en reisdocumenten, met het oog op de afgifte van zulke documenten. Voor de toepassing van deze verordening mogen de biometrische kenmerken in paspoorten en reisdocumenten alleen worden gebruikt voor het verifiëren van:*
*a) de authenticiteit van het paspoort of reisdocument;*
*b) de identiteit van de houder door middel van direct beschikbare vergelijkbare kenmerken wanneer het overleggen van een paspoort of reisdocument wettelijk vereist is."*

Opvallend is dat het gebruik van de biometrische gegevens in de chip expliciet is beperkt tot de hierboven genoemde doelen.

Omdat de specificaties voor het paspoort vanuit de ICAO (Doc 9303) ruimte voor interpretatie laten, is in Europa in april 2006 de BIG opgericht: de Brussels Interoperability Group. Dit is een subcommissie van de Article 6 Committee. Deze

commissie bestaat uit vertegenwoordigers van de lidstaten en vloeit voort uit de implementatie van Artikel 6 van Regulation EC No1683/95 aangaande het invoeren van een uniform format voor visa. De Article 6 Committee heeft als taak de Europese Commissie te assisteren bij het opstellen van aanvullende specificaties voor een uniform format voor een Europees visum, in het bijzonder betreffende technische maatregelen die vervalsing moeten tegengaan. Later is daar het paspoort aan toegevoegd.

Als technische subcommissie van de Article 6 Committee had de BIG de taak om een technische oplossing te ontwikkelen voor de beveiliging van de paspoortchip en de interoperabiliteit van het nieuwe paspoort als geheel. Op de agenda stonden de BAC (Basic Access Control) en de EAC (Extend Access Control). Meer hierover is te lezen verder in dit hoofdstuk. Het uiteindelijke doel van de BIG was om te komen tot een Europese consensus rond de specificaties voor BAC en EAC, alsmede voor het opzetten van tests en pilots. De eerste proeven rond de interoperabiliteit waren overigens nogal bedroevend: meer dan 60% van de paspoorten waren onderling niet uitleesbaar. Een aantal jaar van intensief werk heeft uiteindelijk de grootste problemen opgelost.

De keuze van de ICAO voor de gelaatsscan en voor een facultatieve invoering van de vingerafdruk en/of de irisscan op het niveau van het image is ingegeven door een gebrek aan interoperabiliteit van de templates. Er was bij de ICAO weliswaar een voorkeur voor templates (kleiner bestandsformaat en snellere matching), maar dit was nog niet realiseerbaar. In 2005 heeft het Europese project Minutiae Template Interoperability Testing (MTIT, www.mtitproject.com) in kaart gebracht dat de industrie nog een lange weg te gaan heeft om echte interoperabiliteit te bereiken op het niveau van de templates. Het feit dat dat tot op de dag van vandaag niet is gelukt, heeft voornamelijk twee oorzaken:

- de industrie gebruikt het gebrek aan interoperabiliteit om haar commerciële belangen te beschermen;
- standaardisatie van de kwaliteit van de biometrische images, op basis waarvan de templates worden gegenereerd, ontbreekt doordat er nog geen uniforme test bestaat om de kwaliteit onafhankelijk te evalueren.

Nu er voor images was gekozen kon elk land zijn eigen leverancier kiezen. De wijze waarop de minutiae in een databestand worden opgeslagen is overigens wel gestandaardiseerd, zodat vanaf dat niveau uitwisseling zonder problemen mogelijk is.

Richtlijn EC2252/2004 schrijft onder meer het gelaat én twee vingers voor als verplichte biometrische gegevens, omdat studies hebben aangetoond dat de vingerafdruk beter geschikt is voor het bestrijden van 'look alike fraude'. Dat was de primaire reden voor het toevoegen van biometrische gegevens in de chip van het 'Europese' paspoort. De invoering van de foto van het gelaat en de vingerafdruk zou gefaseerd plaatsvinden.

Aanvankelijk was de chip in het paspoort eenvoudig uitleesbaar, ook op afstand, omdat het een zogenaamde RFID-chip betreft die op afstand uitleesbaar is. Dit leidde tot discussies over privacy en de bescherming van de persoonlijke gegevens die worden opgeslagen in de chip. Om dit probleem op te lossen zijn er twee beveiligingsmethoden ontwikkeld om de persoonlijke data in de paspoortchip te beveiligen tegen ongeautoriseerd uitlezen.:

- De Basic Access Control (BAC): de machineleesbare code onderaan de houderpagina van het paspoort vormt de toegangscode tot de persoonlijke gegevens in de chip (inclusief de foto van het gezicht). Vanaf nu was de chip niet meer uitleesbaar, zonder eerst het paspoort op een daarvoor geschikte scanner te leggen.
- De Extended Access Control (EAC): dit is een op PKI (Public Key Infrastructure) gebaseerde toegangsbeveiliging, waarbij pas na uitwisseling van de juiste certificaten (uitgegeven door de Nederlandse overheid) de vingerafdruk uit de chip gelezen kan worden. Elk land geeft zijn eigen certificaten uit. Om in Nederland de vingerafdruk uit een Duits paspoort te kunnen lezen is dus het Duitse certificaat nodig.

Hoewel binnen Europa de technische aspecten van de EAC lijken te zijn opgelost, blijven er toch nog problemen die een goed functioneren op wereldwijde schaal in de weg staan, om de volgende redenen.

- Niet alle staten hebben genoeg onderling vertrouwen om elkaars certificaten uit te wisselen.
- Het bilateraal uitwisselen van certificaten zorgt op een wereldwijde schaal voor technische problemen (onder andere beschikbaarheid en beveiliging).

Om deze problemen het hoofd te bieden heeft de ICAO recent de zogenaamde PKD opgezet: een centraal vanuit de ICAO beheerde Public Key Directory.

Wat de PKD precies voor impact heeft op de controle over het wereldwijde reisverkeer van personen is voor deze studie niet onderzocht. Omdat het hier om privacygevoelige gegevens gaat (de PKD geeft namelijk een certificaat af waarmee de vingerafdrukken uit de chip gelezen kunnen worden), zou een nader onderzoek nuttig kunnen zijn. Om aan de PKD deel te kunnen nemen dient er een jaarlijkse *fee* te worden betaald. Nog relatief weinig landen hebben zich aangemeld. Zie voor meer informatie hierover de website van de ICAO.[17]

Het interoperabiliteitsprobleem op het niveau van de beveiligingstechniek is (mede door de inspanningen van de BIG) weliswaar grotendeels opgelost, maar inmiddels staat een ander probleem op de agenda: de interoperabiliteit op applicatieniveau, met 'image quality' als centraal onderwerp. Vanwege gebrek aan standaards en afspraken op dit punt gaan lidstaten daar verschillend mee om. Dat gaat om de beoordeling van de kwaliteit bij de registratie, maar ook om de beslissing om slechte images al dan niet op te slaan in het paspoort en wat dan de drempelwaarden moeten zijn.

In 2009 heeft de BIG zijn werk afgerond. De operationelere vraagstukken rond de interoperabiliteit van het biometrische paspoort in Europa staan inmiddels op de agenda van Frontex, een onafhankelijk Europees agentschap met als taak de samenwerking tussen de Europese lidstaten op het gebied van grensbewaking te coördineren.[18] Dat de kwaliteit van de gezichtsopname en vingerafdrukken een belangrijk onderwerp zijn blijkt uit de verordening (EG) Nr. 444/2009 van het Europees Parlement en de Raad van 28 mei 2009, waarin is besloten tot een aantal wijzigingen van Verordening (EG) nr.

17 www2.icao.int/en/MRTD/Pages/icaoPKD.aspx.
18 ww.frontex.europa.eu/.

2252/2004. Die houden onder andere in dat er voor reisdocumenten aanvullende kwaliteitseisen en gemeenschappelijke technische normen inzake gezichtsopname en vingerafdrukken moeten komen.

Deze wijziging heeft direct te maken met het gebrek aan mogelijkheden om op uniforme wijze de kwaliteit van biometrische images te testen en te valideren. Meer gedetailleerde informatie over deze problematiek wordt beschreven in de volgende paragrafen.

### *5.2 ISO-standaarden*

Nadat de ICAO rond 2000 was begonnen met het standaardiseren van biometrie voor het paspoort, is er gelijktijdig een versnelling opgetreden in de standaardisatie van de verschillende biometrische componeneten. Dat heeft geleidt tot de SC37, een werkgroep die onder ISO valt. Het gaat om de volgende categorieën.

- Biometric Technical Interface Standards.
- Biometric Data Interchange Format Standards.
- Biometric Performance Testing and Reporting Standards.
- Conformance Testing Methodology Standards.[19]

Voor de vingerafdruk is de standaard ISO-standaard 19794-4 relevant. Deze regelt de metadata met betrekking tot kwaliteit om het management van de kwaliteit te regelen, maar *niet de kwaliteit zelf*. Daar is vaak verwarring over. Hoewel veel standaards in een vergevorderd stadium dan wel afgerond zijn, is een aantal relatief recent opgestarte standaards die betrekking hebben op de image quality nog volop in ontwikkeling. Vanwege het belang van de beoordeling van de vingerafdrukkwaliteit voor het meten en verbeteren van de prestaties van operationele systemen, hebben leveranciers hun eigen kwaliteitsalgoritmen ontwikkeld en toegepast. Bij grote projecten zoals US-VISIT (www.dhs.gov/us-visit), PIV (Personal Identity Verification of Federal Employees and Contractors, FIPS 201) and the EU-VIS/BMS (2006/648/EC) is het meten en rapporteren van kwaliteitsscores van de opgenomen images verplicht. Kwaliteit is dan ook een onderwerp van veel onderzoek, resulterend in een set nieuwe standaards (ISO/IEC 29794

19 www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_tc_browse.htm?commid=313770.

serie) die tot doel hebben te komen tot een uniforme interpretatie en evaluatie van kwaliteit en interoperabiliteit van kwaliteitsscores.

De tabel hieronder geeft een overzicht van deze standaards. De standaards 29194 tot en met 29197 hebben betrekking op het biometriesysteem als geheel (dus inclusief processen, procedures en omgevingsfactoren) en bevinden zich nog in een vroeg stadium. De standaards 29794-1, -4 en -5 hebben betrekking op de image quality. Ze zijn weliswaar verder dan de voornoemde standaards, maar bevinden zich nog in de reviewfase. Er zal nog zeker een paar jaar overheen gaan voordat deze standaards in de praktijk toegepast en getest kunnen worden, onder andere omdat daar gevalideerde databases voor nodig zijn.

| ISO Standaard id. | Omschrijving | status ** |
|---|---|---|
| ISO/IEC NP TR 29194 | Guidance on the Inclusive Design and Operation of Biometric Systems | 10.99 |
| ISO/IEC NP TR 29195 | Passenger Processes for Biometric Recognition in Automated Border Crossing Systems | 10.99 |
| ISO/IEC NP TR 29196 | Guidance for Biometric Enrolment | 10.99 |
| ISO/IEC NP 29197 | Evaluation Methodology for Environmental Influence in Biometric Systems | 10.99 |
| ISO/IEC NP 29198 | Biometrics – Characterization and measurement of difficulty for fingerprint databases for tehcnology evaluation | 10.99 |
| ISO/IEC 29794-1:2009 | Information technology – Biometric sample quality – Part 1: Framework | 60.60 |
| ISO/IEC TR 29794-4:2010 | Information technology – Biometric sample quality – Part 4: Finger image data | 60.60 |
| ISO/IEC TR 29794-5:2010 | Information technology – Biometric sample quality –Part 5: Face image data | 60.60 |

*** 10.10 betekent in voorstelfase, 100.100 betekent afgerond; alles ertussen betekent in ontwikkeling*

*Figuur 13: overzicht meest recente ISO-standaards voor biometrie, www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_tc_browse.htm?commid=313770*

Omdat deze standaards nog niet definitef zijn, kunnen ze nog niet worden getest. Tot die tijd is de beste benadering om alles te doen wat mogelijk is om de kwaliteit van de afgenomen vingerafdrukken te optimaliseren met de beschikbare quality assessment tools, zoals het NFIQ van NIST.

### *5.3 BioAPI*

Een standaard die al vroeg naar voren kwam is de BioAPI: Biometric Application Programming Interface. Van deze standaard bestaan twee versies: de ANSI/INCITS 358-2002 (ook wel BioAPI 1.1) en de ISO/IEC 19784 serie (ook wel BioAPI 2.0). Deze industriële standaard maakt het mogelijk dat toepassingen gebruik kunnen maken van biometrische producten van verschillende leveranciers. De beperking van deze standaard is dat het de softwarematige communicatie met de producten regelt (zoals het aanroepen van functies), maar niet de eigenschappen van de biometrische informatie zelf. Dat betekent dat biometrische apparatuur, die BioAPI compliant is, onderling vrij eenvoudig verwisseld kan worden zonder dat de gehele applicatie opnieuw geprogrammeerd hoeft te worden. Helaas zorgt de standaard niet voor goede kwaliteit plaatjes en ook niet dat leveranciers met elkaars templates kunnen werken. Ondanks de BioAPI is de kans nog steeds groot dat bij het wisselen van leverancier toch van iedereen opnieuw de biometrische gegevens moeten worden afgenomen. Zeker voor grootschalige toepassingen is dat zeer onwenselijk, zo niet onmogelijk. Het verwijzen naar de BioAPI-standaard is dus onvoldoende om een toepassing veilig te stellen voor een ‘vendor lock in’. Ook zegt conformiteit met de BioAPI-standaard niets over de prestaties van het biometrische systeem als geheel, noch van de componenten afzonderlijk.

### *5.4 Rol van universiteiten*

Het gebrek aan standaards en de opkomst van de biometriemarkt heeft geleid tot een sterke impuls bij universiteiten om onderzoek te starten op het gebied van biometrie. Dat gebeurt dan ook op grote schaal. Vrijwel alle relevante universiteiten in Europa en daarbuiten hebben biometrie op de een of andere wijze in hun curricula verwerkt. Binnen Europa zijn de universiteiten van Twente, Kent, Brnö, Bologna, Barcelona, Darmstadt, Gjøvik en Tilburg hiervan goede voorbeelden. Het betreft overigens niet alleen de technische richtingen: ook juridische en sociaal-maatschappelijke faculteiten besteden steeds meer aandacht aan de opkomst van biometrie, zoals TILT (Tilburg Institute for Law, Technology and Society) van de universiteit van Tilburg, JMCE (Jean Monnet Center of Excellence) van de universiteit van Leeds en de juridische faculteit van de Universiteit van Leuven.

Er is wel een onderscheid tussen de technische en niet-technische richtingen in de mate waarin zij actief betrokken raken bij de huidige marktontwikkelingen op een uitvoerend niveau. De technische faculteiten leveren over het algemeen meer fundamenteel onderzoek. Dat mondt uit in een veelheid aan nieuwe (al dan niet gepatenteerde) technische ideeën en methoden. Om die uiteindelijk gerealiseerd te zien in de markt zijn vele jaren van ontwikkeling en behoorlijke investeringen nodig. De sociaal-maatschappelijke studies daarentegen (en zeker die betrekking hebben op zaken als privacy, dataprotectie, beleid en wetgeving) vinden makkelijker hun weg. Er zijn immers geen kostbare financieringen voor nodig om een studie of rapportage op te leveren, terwijl beleidsmakers er direct gebruik van kunnen maken. Het is om die reden dat universiteiten regelmatig betrokken zijn bij de beleidsmatige aspecten van biometrietoepassingen. Hoe nuttig ook voor het ontwikkelen van meer begrip en strategische visies, het toepassen van biometrie heeft ook vele praktische aspecten en daar hebben universiteiten veelal wat minder ervaring mee. Het risico van universitaire studies is dan ook dat ze in de praktijk als theoretisch worden ervaren en daarom niet altijd de gewenste uitwerking hebben op de beleidsmakers.

Bij de adoptie van technische vindingen lopen we tegen het probleem aan dat eerder in deze studie is beschreven over de nieuwe biometriebedrijven: hoewel de toepassingsmogelijkheden enorm lijken en in theorie ook zijn, blijft de

daadwerkelijke vraag naar innovatieve biometrieprodukten beperkt. Het naar de markt brengen van nieuwe vindingen en ideeën is daarom een uitdaging. De grootste vraag naar innovatie bevindt zich in de bestaande markt, zoals nationaal identiteitsmanagement, grenscontrole, luchthavenbeveiliging en toegangscontrole. Voor deze markt is men het er in het algemeen over eens dat de volgende onderwerpen de aandacht verdienen van academische en industriële onderzoekers.

- Het verbeteren van de toegankelijkheid en ergonomie van biometrische sensoren en kiosken (onder andere voor het verlagen FRR en het toegankelijk maken voor minder validen).
- Het verbeteren van de prestaties van zoek- en vergelijkingsalgoritmen (sneller, betrouwbaarder).
- 'Spoofing' detectie (het detecteren van een valse vinger, iris, gezicht etc., ook wel 'life detection').
- Nieuwe modaliteiten (3D Face, key stroke, vein pattern, behavioural biometrics, ...).
- Multimodale software en hardware (combinaties van meerdere biometrische technieken).

Om investeringen in bovenstaande innovaties te verantwoorden zullen eerst de aard en omvang van de toegevoegde waarde ervan in kaart gebracht moeten worden. Dat hangt weer af van de vraag in de markt. Daarbij kijken we direct in de richting van de belangrijkste klant van biometrische producten op dit moment: de overheid. Het lastige is dat juist deze klant zo zoekende is naar het helder krijgen van haar eisen en behoeften. Mede dat gebrek aan helderheid staat een gezonde vraag naar innovatie in de weg.

## 6. Testen van biometrische componenten en systemen

In dit hoofdstuk wordt ingegaan op de toetsing van de techniek en het proces. Ondanks de diverse standaards blijkt het onafhankelijk testen van biometrische producten en systemen nog een lastige zaak. Biometrische software en hardware worden weliswaar regelmatig getest, maar het adequaat testen van een end-to-end biometrisch systeem in operationele omstandigheden is maar zelden gedaan. Door een gebrek aan uniforme

testmethodes zijn de resultaten van verschillende tests maar moeilijk met elkaar te vergelijken.

### *6.1 Interoperabiliteit en 'vendor lock-in': BioTesting Europe 2007*

BioTesting Europe is een door de Europese Commissie gefinancierd onderzoek naar de mogelijkheden van het ontwikkelen van Europese competenties op het gebeid van testen en certificeren van biometrische componenten en systemen. Het project is uitgevoerd door het European Biometrics Forum met als partners Fraunhofer (D), national Physical Laboratory (UK)me het European Joint Research Center (EC JRC). De resultaten zijn te vinden op www.biotestingeurope.eu.

Tot op heden hebben grootschalige vingerafdruksystemen, ondanks de vele tientallen jaren dat de vingerafdruktechniek wordt gebruikt, te leiden onder een gebrek aan interoperabiliteit op het niveau van de image quality en het bepalen van de biometrische kenmerken (zoals de minutiae van vingerafdrukken).

> *"The existing standardisation work on biometrics defines fingerprint image quality as well as minutiae placement. However, the precision with which these minutiae points are located leave room for proprietary interpretation. This causes an overall lack of interoperability between the vendors of fingerprint capturing and encoding software, despite available standards. The result is a biometric market, which is dominated by proprietary products, high costs of ownership, an inefficient use of the systems and lower security performance. Large projects such as the new biometric passports, the European Biometric Matching System (BMS) and US VISIT are severely suffering from this in terms of lower performance, higher costs and therefore lower Return on Investment."* [20]

Dit citaat komt uit de eindrapportage van BioTesting Europe, een door de Europese Commissie gefinancierd project dat laat zien dat onafhankelijk onderzoek de enige manier is om leveranciersonafhankelijke referenties en testinstrumenten te ontwikkelen. Daardoor kunnen bijvoorbeeld image quality en juiste plaatsing van de minutiae getest worden ten opzichte van de bestaande standaards. Thans produceren leveranciers

20 Final Report Biotesting Europe, www.biotestingeurope.eu.

verschillende templates op basis van een en hetzelfde plaatje van een vingerafdruk, zelfs als iedereen verwijst naar dezelfde standaards. Als gevolg daarvan zijn de prestaties van een biometrisch systeem in de praktijk pas optimaal als de technologie van een enkele leverancier wordt gebruikt voor zowel de kwaliteitsanalyse van het plaatje als het genereren van de features. Dit veroorzaakt een intrinsieke 'vendor lock-in', een situatie die zeker voor grote toepassingen onwenselijk is. Verdere conclusies van BioTesting Europe zijn de volgende.

- *Independent testing and certification will improve the overall trust of biometric systems.*
- *According to stakeholders the most relevant and urgent areas to be tested and certified are:*
    - *Interoperability (especially Image interoperability).*
    - *Performance (mainly failrure to enrol / false acceptance / rejection).*
    - *Security (spoofing).*
    - *Ergonomics and human aspects (enrolment and verification process, kiosks, etc.).*
- *Lack of knowledge and experience leads to unclear requirements and costs situation. The results are:*
    - *Vendor driven pricing.*
    - *High prices because vendors include risks and costs for benchmarking and pre-tests.*
- *Independent testing will significantly lower the short term and long term costs of biometric procurements, because there will be:*
    - *Less vendor dependency.*
    - *Clearer pricing and costs structure.*
    - *Lower integration costs*[21].

Alle resultaten zijn te vinden op www.biotestingeurope.eu.

21 Idem.

### *6.2 Independent vs in-house testing*

Met 'independent testing' wordt bedoeld het testen door gecertificeerde testlaboratoria, zoals het NPL in de UK en TNO in Nederland. Deze laboratoria zijn in staat om professionele testprogramma's te ontwikkelen. De tegenhanger ervan is 'in-house testing'. Daarbij test de eindgebruiker/klant zelf zijn eigen beoogde toepassing of delen daarvan. Aan beide methoden zitten voor- en nadelen.

| | **Voordelen** | **nadelen** |
|---|---|---|
| **in-house testing** | De klant leert zijn eigen systeem en technologie kennen.<br><br>Operationele omstandigheden kunnen makkelijker worden meegenomen.<br><br>Kennis wordt opgebouwd binnen de de organisatie. | Wanneer eindgebruiker niet over de juiste kennis beschikt wordt de test onbetrouwbaar.<br><br>Politieke dan wel interne krachtenvelden kunnen afbreuk doen aan de onafhankelijkheid en transparantie van de test. |
| | | |
| **independent testing** | Onafhankelijke testlaboratoria hebben de juiste kennis en ervaring.<br><br>Minder kans op beïnvloeding door politieke en andere factoren.<br><br>De klant wrodt gedwongen over zijn specificaties na te denken. | Uitkomsten zijn niet altijd wat de klant wil horen.<br><br>Niet alle operationele omstandigheden kunnen altijd worden meegenomen.<br><br>Risico op theoretische uitkomsten. |
| | | |

*http://www.eubiometricsgroup.eu/*

Interessant om te noemen zijn ook de recente uitkomsten van het al eerdergenoemde BioDev testprogramma (zie 'Folder BioDev II_UK 21-7-2007'). Dit programma is ontwikkeld om het biometrische aanvraagproces voor een Europees visum op consulaire

posten te analyseren en te optimaliseren. Het Europese visumaanvraagproces is gebaseerd op het Visa Information System, binnenkort ondersteund door het Biometric Matching System (BMS). Dit centrale systeem vraagt bij elke aanvraag de tien vingers van de aanvrager. Daarmee wordt eerste gekeken of de persoon zich al eerder heeft aangemeld bij een ander consulaat, al dan niet onder dezelfde naam. Bij een nieuwe aanvraag worden de afdrukken van alle tien de vingers centraal opgeslagen in het BMS. Bij controle aan de grens wordt aan de hand van het visanummer en vier vingers geverifiëerd of de persoon daadwerkelijk bij het visum hoort. BioDev behelst alleen het aanvraagproces. Er is nog geen technische infrastructuur voor het verificatieproces. Een belangrijk aspect van het VIS/BMS is dat alle Europese landen hierop zijn aangesloten en dat de centrale database van het BMS dus data ontvangt die door verschillende biometrische leveranciers zijn gegenereerd. Het eerder besproken probleem van uniforme kwaliteitsanalyse gecombineerd met beoogde hoge prestaties levert een uitdaging op voor de beheerders, die om de prestaties te optimaliseren niet onder een bepaalde kwaliteitsnorm kunnen werken. Alleen die norm is zoals gezegd niet voor alle leveranciers hetzelfde.

### *6.3 BioDev: een enrolmentproef voor consulaten en ambassades 2005 - 2010*

Parallel aan het nieuwe EU VIS zal de Europese Commissie een centraal vingerafdruksysteem gaan inrichten ten behoeve van het controleren van de identiteit van de aanvragers van een Europees visum: het Biometric Matching System (BMS). Om te bekijken wat de impact daarvan is op het aanvraagproces en om te kijken of het BMS in staat is om de vingerafdrukken van diverse consulaten (en van diverse leveranciers) te verwerken, heeft een aantal lidstaten besloten om een operationele proef te doen: BioDev.

Om beter te begrijpen waar BioDev over gaat volgt eerst een korte uitleg over het BMS. De bedoeling van het BMS is dat bij elke visumaanvraag de tien vingers van de aanvrager worden afgenomen en opgeslagen. Na de afname wordt eerst in het BMS aan de hand van de vingerafdrukken gecontroleerd of de aanvrager al eerder een visum heeft aangevraagd onder dezelfde of een andere naam. Dit is een 1:n vergelijking. Omdat dit op alle consulaire posten van alle Europese lidstaten gebeurt, wordt het zogenaamde ‘visa

shopping' daarmee tegengegaan. Dat wil zeggen dat wordt voorkomen dat mensen meerdere aanvragen doen voor verschillende landen, al dan niet met verschillende identiteiten. Als het visum wordt toegekend, krijgt de aanvrager een sticker met een uniek nummer in zijn paspoort. Bij controle aan de Europese grens worden vier vingers van de reiziger afgenomen en wordt het nummer van de visumsticker gelezen. Dat nummer fungeert als verwijzing in het BMS en haalt de biometrische gegevens van de persoon op. Die worden geverifiëerd met de reiziger. Dit is een 1:1 vergelijking.

Alle lidstaten zijn in de toekomst aangelsoten op het BMS. Maar niet alle lidstaten hebben dezelfde biometrieleverancier als het BMS. Dat betekent dat biometrische plaatjes van verschillende leveranciers in het systeem moeten worden opgeslagen. Echter, wat voor het BMS een goede kwaliteit is, beoordeelt een andere leverancier als onvoldoende. Voor het BMS mogen de plaatjes van bepaalde leveranciers (en dus in dit geval van bepaalde lidstaten) niet op grote schaal en structureel geweigerd worden. Dat levert logistieke problemen op bij de betreffende consulaten. Bovendien haalt een hoge FTE het principe van het systeem onderuit. Een brede acceptatie van de plaatjes is dus noodzakelijk. Om bij een grote variatie in de kwaliteit een lage FRR te krijgen zal de drempelwaarde voor de kwaliteit omlaag moeten. Maar dat levert weer uitdagingen op voor het verkrijgen van de gewenste FAR voor het centrale systeem. Dus: een lage kwaliteitsdrempel levert weliswaar een lage FRR op de consulaten, maar zorgt bij het BMS voor een groter aantal hits. Die moeten dan weer nader onderzocht worden door experts en dat is niet de bedoeling: het BMS is zodanig gespecificeerd dat het slechts één hit mag opleveren. Is de kwaliteitsdrempel van het BMS hoog, dan wordt de FRR op de consulaten hoog waardoor er vertragingen ontstaan bij consulaten.

BioDev is een proef van een aantal lidstaten (AT, BE, DE, FR (project manager), LU, PT, ES en UK) met betrekking tot de registratie en verwerking van de vingerafdrukken op de consulaire posten van Europese lidstaten. Gezien de hierboven beschreven problematiek is het niet verbazend dat BioDev zich voor een groot deel heeft gericht op de kwaliteit van de vingerafdrukken. Immers, zowel de FRR als de FAR profiteert van goede kwaliteit van de afdrukken.

Tijdens een presentatie op 2 maart 2010 tijdens de Biometrics Consortium Conference in Gaitherbrough (US) presenteerden Fares Rahum (German Federal Office of Administration, BV.A) en Oliver Bausinger (German Federal Office for Information Security, BSI) de volgende resultaten naar aanleiding van metingen op twee consulaire posten in respectievelijk Damascus en Ulan Bator.[22]

- Fundamental: use high quality capture device
- Better quality of fingerprints yields to better AFIS performance.
- Use only fingerprints of a certain quality level: Enrolment performance is predicted by the Sagem quality control USK 4.
- Quality for the VIS practically means Sagem USK 4 quality.
- Quality assurance has a large impact on the overall process.
- Good quality can only be achieved as a combination of operational and software-based quality measures.
- High quality comes at a price (enrolment time, scanners).
- You can learn how your system works if you have enough logging data!
- Need for specifying best practices for high quality enrolment processes.
- Improvements of local rejection rate from Fase 1 to Fase 2:

| | **Damascus** | **Ulan Bator** |
|---|---|---|
| Phase 1 | 69% | 82% |
| Phase 2 | 25% | 43% |

- Improvements of central rejection rate from Fase 1 to Fase 2:

| | **Damascus** | **Ulan Bator** |
|---|---|---|
| Phase 1 | 16% | 15% |
| Phase 2 | 3% | 3% |

22 Presentatie: *Best Practice Fingerprint Enrolment Standards European Visa Information System: Improving performance by improving fingerprint image quality - Experiences from pilot project BioDEVII,* beschikbaar op: http://biometrics.nist.gov/cs_links/ibpc2010/pdfs/Rahmun_Fares_BausingerOliver_20100303_BestPracticeFingerprintEnrolmentVIS.pdf

Verdere conclusies zijn de volgende.

- Ondanks een grote verbetering zijn de lokale rejection rates nog steeds significant.
- Verbeterde kwaliteitsanalysesoftware (zgn. Kit4) heeft de centrale rejection rate aanzienlijk verlaagd, maar roept wel vragen op met betrekking tot de afhankelijkheid van een enkele leverancier (i.c. Sagem) en de gevolgen van de nog steeds hoge lokale rejection rate.
- Operationele omstandigheden, kwaliteit apparatuur en de vaardigheden van de baliemedewerkers zijn essentiëel voor het verkrijgen van optimale kwaliteit.

### *6.4 Germany Puts Quality First 2009*

Mede vanwege de bevindingen van BioDev heeft de Duitse overheid ervoor gekozen zich in de eerste plaats te richten op de kwaliteit van het regitratieproces. Het artikel 'Germany Puts Quality First' door Uwe Siedel, gepubliceerd in de 29ste editie van het *Keesing Journal of Documents and Identity* in 2009, beschrijft hoe de Duitse overheid dit heeft aangepakt. Omdat dit tijdschrift alleen voor leden beschikbaar is, volgt hier een overzicht van de belangrijkste punten.

- Er is een centrale database aangelegd voor uitsluitend het opslaan en analyseren van de kwaliteitsscores van alle vingerafdrukken: het CQAR, Central Quality Assurance Respository. De vingerafdrukken zelf worden dus niet in een centrale database opgeslagen.
- Er zijn kwaliteitscriteria opgesteld voor de enrolment van vingerafdrukken en gezichtsopnames.
- Onder kwaliteit wordt in deze context verstaan de mate waarin de afgenomen biometrische gegevens voldoen aan van tevoren gestelde specificaties.
- Een zorgvuldig uitgebalanceerd enrolment proces is minstens net zo belangrijk voor de kwaliteit als de enrolment hardware.
- De biometrische en andere persoonlijke gegevens worden niet in een centrale database opgeslagen.
- Het enrolment proces is 'quality centered'.

In de tabel hieronder staan de kwaliteitsscores van de vingerafdrukken va ca. 1.000.000 paspoortaanvragen, afkomstig uit de CQAR en gemeten tussen juli en december 2008.

| NFIQ | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| % | 73% | 17,6% | 7% | 1,6% | 0,7& |

1 = hoogste kwaliteit

5 = laagste kwaliteit

Overigens is voor de Duitse National e-ID-kaart het opslaan van de vingerafdrukken optioneel. Ook daarvoor geldt dat de wetgeving voorziet dat de vingerafdrukken niet in een database worden opgeslagen.[23]

### *6.5 Benchmarking: BMS en het Indian UID-project*

*"Een benchmark, vertaalbaar als 'referentiekader' of 'ijkingskader', is een basis om de prestaties van verschillende systemen, apparaten of organisaties met elkaar te kunnen vergelijken."*[24]

Onder invloed van internationale samenwerking en de ontwikkeling van grootschalige biometriesystemen staat het systeem van nationale verkaveling onder druk. Waar eerst een leveranciersafhankelijk biometriesysteem niet direct tot interoperabilteitsproblemen leidde, doet het dat nu wel, omdat paspoorten internationaal uitleesbaar moeten zijn en Europa vanuit al haar consulaire posten het Europese BMS van tientallen miljoenen vingerafdrukken moet gaan voorzien (zie ook paragraaf 6.3 betreffende BioDev). Doordat er tot op de dag van vandaag geen eensluidende interpretatie van bepaalde relevante standaards is, waaronder die voor image quality en de plaatsing van de minutiae, is het lastig om uniforme tests uit te voeren op de verschillende producten. Bij onvoldoende en/of onvolwassen standaards is een benchmark een goed alternatief. Je

23 Zie http://www.bundesregierung.de/Content/DE/Artikel/ArtikelNeuregelungen/2010/2010-10-26-gesetzliche-neuregelungen.html.

24 www.wikipedia.com.

laat verschillende leveranciers een systeem bouwen en die ga je onderling vergelijken. De klant doet de benchmarktest bij voorkeur zelf, omdat hij dan beter kan bepalen of het systeem in functionele zin doet wat hij wil. Bovendien kan hij dan ook de operationele aspecten beter vergelijken.

Een andere reden voor overheden om zelf hun tests te doen is omdat ze zodoende zelf het systeem en de technologie beter leren begrijpen, op basis waarvan ze later beter in staat zijn hun eisen te formuleren en eventueel aan te besteden. Testinstituten en universiteiten worden regelmatig betrokken bij dit soort tests, onder andere om te helpen bij het opstellen van de juiste methodiek en het beoordelen van de resultaten. Bij gebrek aan standaards kan een benchmark voor de klant dus leiden tot meer inzicht in zijn eigen eisen en tot een beste keus op basis van operationele argumenten. Het nadeel van een benchmark is dat het niet altijd inzichtelijk is hoe een bepaald product of systeem tot zijn prestaties komt. Bovendien kan die inzichtelijkheid per leverancier verschillen.

In de wereld van grote biometriesystemen is benchmarking een veelgeziene vorm voor het testen en selecteren van leveranciers. De bestaande ISO-standaards zijn relatief nieuw en zijn zeker voor end-to-end systemen (nog) niet geschikt. Er zijn immers veel niet-technische factoren die de prestaties van het systeem als geheel beïnvloeden. Dat betekent dat een afnemer niet uitsluitend kan terugvallen op testbare standaards als criterium voor het evalueren en controleren van bepaalde claims rond prestaties en conformiteit. Zeker als de klant zelf geen ervaring heeft met het systeem dat hij wil aanbesteden en daarenboven ook zijn eigen systeemeisen niet in detail kent, dan wordt benchmarken de enige optie.

Aangezien de Europese lidstaten verschillende Programma's van Eisen hebben (onder andere als gevolg van verschillende juridische implementaties van EC2252/2004), is het risico groot dat elk land voor zichzelf de tests en benchmarks doet en dat de uitkomsten daarvan niet altijd onderling vergelijkbaar zijn. Dat vormt een zeker risico wanneer je als Europese lidstaat voorop wil lopen: de kans dat in een later stadium de eisen en criteria veranderen vanwege de noodzaak van internationale interoperabiliteit is altijd aanwezig.

Het Biometric Matching System (BMS) van de Europese Commissie (zie ook paragraaf 6.3), onderdeel van het Visa Information System (VIS), is een goed voorbeeld van een aanbesteding via een benchmark. Om een leverancier te selecteren heeft de commissie een functioneel Programma van Eisen opgesteld met een aantal criteria voor de prestaties (onder andere FAR, FRR, snelheid). Vervolgens heeft een viertal leveranciers een werkende demoversie gebouwd. Door de prestaties onderling te vergelijken is er een beste keus vastgesteld. De prijs heeft daarbij een belangrijke rol gespeeld.

Het grootste benchmarkproject voor een biometrisch systeem van dit moment is ongetwijfeld het Indiase Unique Identity Project (IUID: http://uidai.gov.in/), waarbij de gehele Indiase bevolking (circa 1,2 miljard personen) in een centrale database zullen worden geregistreerd (inclusief twee irissen en tien vingers). Voor deze megabenchmark zijn er vijf leveranciers uitgekozen op basis van een voorselectie. Daarvan gaan er drie het systeem met complete functionaliteit bouwen en uitrollen in voor elk een eigen geografisch gebied. De partij die uiteindelijk het beste presteert krijgt de opdracht.

Een nadeel van een benchmark zijn de kosten: indien niet voor de afnemer, dan wel voor de leverancier. In het geval van de IUID moeten drie partijen het gehele systeem gratis bouwen én operationeel uitrollen. Uiteindelijk krijgt slechts één partij betaald. De andere partijen hebben dan enkele miljoenen geïnvesteerd. Voor de industrie is dat een kostbare kwestie. Uiteraard zullen deze kosten uiteindelijk door de markt betaald moeten worden. Daarnaast verhoogt deze grote en nogal riskante investering de toegangsdrempel voor nieuwe partijen.

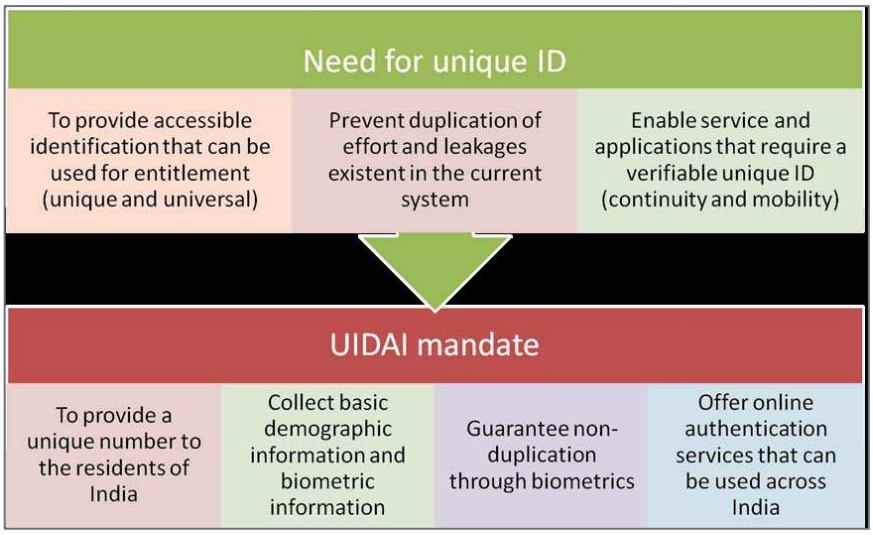
Als voorbereiding op de benchmark heeft het IUID-project een uitgebreide technische studie naar de biometrie gedaan, gepubliceerd in een uitgebreide publieke rapportage: *Biometrics Standards for UID Applications*.[25]

Deze studie is uitgevoerd door de speciale UIDAI Committee on Biometrics, waarbij de leden van de commissies en subcommissies met naam en toenaam staan genoemd. De studie gaat op doortastende wijze in op zaken als kwaliteit, prestaties en operationele omstandigheden. Het gaat daarbij geen uitspraken uit de weg met betrekking tot

25 Zie http://uidai.gov.in/UID_PDF/Committees/Biometrics_Standards_Committee_report.pdf.

factoren die een negatieve invloed kunnen hebben op de kwaliteit van de afgenomen biometrische gegevens. Door de openheid waarmee het rapport is geschreven en ter beschikking is gesteld bestaat er een algemeen niveau van begrip van de mogelijkheden en uitdagingen van het ontwikkelen van een dergelijk systeem. Het gevolg is dat zaken in brede kring besproken kunnen worden, hetgeen bijdraagt aan een heldere en open discussie.

Overigens is de functionaliteit van het IUID-project beperkt tot de-duplicatie: het (off line) detecteren van meerdere registraties van één persoon. De belangrijkste functie van het IUID-project is het registreren van de gehele bevolking en het toekennen van een uniek 12-cijferig identiteitsnummer aan alle burgers (inclusief kinderen). Het systeem wordt een universele identiteitsinfrastructuur, waarmee alle burgers toegang krijgen tot zowel overheids- als commerciële diensten. Er wordt geen id-kaart uitgegeven en registratie is vrijwillig. In de onderstaande figuur staan de doelstelling in een overzicht.

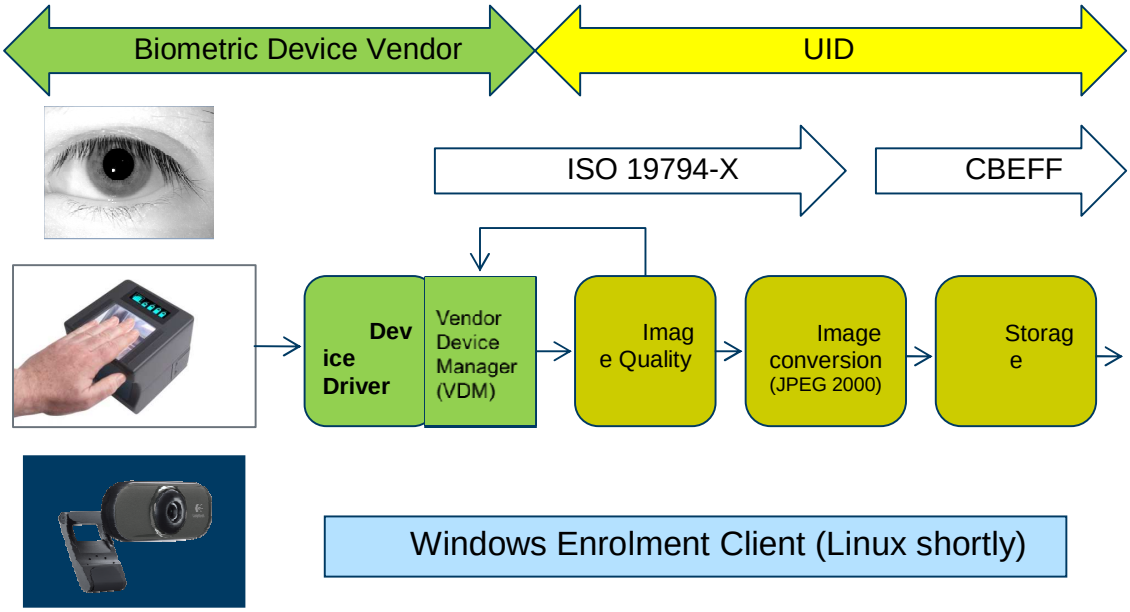



*Figuur 14:..... doel Indian UID*[26]

Bij de specificatie van het biometrische systeem is er zoveel mogelijk gebruikgemaakt van de bestaande standaarden. Voor de image quality heeft IUIDA een eigen maatstaf ontwikkeld, omdat de serie ISO 29794-x nog niet voldoende is gevorderd. Voor het

26 Figuur afkomstig uit een presentatie gehouden door Tim Pigeon van L1 Identity Solutions (http://www.l1id.com) tijdens het 6th EBF Seminar, Brussel 4 november 2010. De presentatie is te vinden op www.eubiometricsforum.com.

testen van de conformiteit met deze standaarden zijn onafhankelijke partijen ingeschakeld. Hiermee wordt bereikt dat de drie gekozen leveranciers beter met elkaar zijn te vergelijken. De volgende figuur geeft in hoofdlijnen de gekozen standaards weer.




*Figuur 14: Standaards in het Indian UID Project*[27]

### *6.6 Testelementen voor een end-to-end systeem: het belang van goede enrolment*

Als wij greep willen krijgen op de prestaties van een op biometrie gebaseerd end-to-end systeem, dan kunnen we niet anders dan alle tussenliggende elementen definiëren en specificeren in kwantificeerbare en evalueerbare grootheden. Bij een bevolkingsadministratie begint dat bij de aanvraag en uitgifte van een identiteitsdocument en de afname van de biometrisch gegevens. Zoals al meerdere malen besproken in deze studie, zijn de kwaliteit en integriteit van de biometrische gegevens door de gehele identiteitsketen van groot belang. Om de kwaliteit en

27 Idem.

integriteit zowel direct als op langere termijn te kunnen waarborgen betekent dat voor het biometrische gedeelte dat de volgende checklist een vereiste is.

- Hoeveel pogingen worden er gedaan per vinger.
- Waardoor zijn de pogingen mislukt.
- Wat is de uiteindelijke kwaliteit van de opgenomen vingerafdrukken.
- Heeft er verificatie plaatsgevonden.
- Is er ook geverifieerd met de gegevens in de database.
- wat waren de kwaliteit- en matchingscores.
- Hield de aanvrager zijn/haar vingers goed op de sensor.
- Waren de omstandigheden optimaal (oa. plaatsing en toestand van de sensor).
- Was het geen nep-vingerafdruk.
- Heeft de persoon niet moedwillig zijn/haar vingerafdruk onbruikbaar gemaakt.
- .....

In deze lijst zitten elementen die automatisch door het systeem gemeten en gelogd kunnen worden, maar ook elementen waarvoor menselijk optreden ter plaatse en/of achteraf nodig is. Dat kan gedeeltelijk door het baliepersoneel gebeuren, maar voor bepaalde taken is dat niet mogelijk. Dat kan zijn omdat de baliemedewerker daar geen tijd of de juiste kennis voor heeft, maar ook omdat nader onderzoek bepaalde autorisatie vraagt en gedeeltelijk misschien off line moet plaatsvinden. Als biometrie een bijdrage moet leveren aan het terugdringen van fraude met identiteitsdocumenten, dan moeten er procedures zijn om bij de aanvraag van een reisdocument te kunnen beoordelen of mislukte verificatie bij uitgifte terecht of onterecht is. En andersom: of een gelukte verificatie wel tot stand is gekomen op basis van integere gegevens. Daarbij moet een onderscheid gemaakt kunnen worden tussen fouten van het systeem zelf en fouten die bewust zijn opgeroepen door de persoon die het reisdocument heeft aangevraagd.

Marek Rejman Greene, Senior Biometrics Adviser van de Scientific Development Branch van de UK Home Office en initiatiefnemer van het nog in ontwikkeling zijnde

document ISO/IEC WD 29196 Guidance for Biometric Enrolment, stelt voor de kwaliteitsbewaking van het registratieproces onder andere het volgende voor.

*"Examples of metrics which the Authority may wish to consider including in a SLA (Service Level Agreement) are:*

- *Performance statistics from the Relying Party operating a service which is dependent on a successful enrolment of subjects, with a breakdown to help identify the impact of any variations in quality of the enrolment service.*
- *User satisfaction statistics, for example, extracted from analysis of questionnaires, numbers of complaints from enrolees or assessment from media reports*
- *Identity proofing failure rates.*
- *Failure to Enrol rates, analysed by demographic group, enrolment centre, time of day, the type of resolution procedure which was applied and the results of such actions.*
- *Distributions of image and enrolment quality, analysed by demographic group, enrolment centre, time of day, etc.*
- *Number of retries required and whether or not an operator override (e.g. of quality threshold) was used.*
- *Statistical measures relating the duration of biometric enrolment (e.g. mean time from start of the process through to successful conclusion, maximum response times from a central database - if a check for duplicate enrolments is made).*
- *Proportion of enrolments which fail the verification test (for services where these are implemented).*
- *Transaction logging of appropriate granularity.*
- *Auditing support consistent with a set of established requirements."*[28]

28 6th EBF Seminar, 4 november 2009, http://www.eubiometricsforum.com/.

## 7. Conclusies Deel II

De internationale markt voor biometrische producten wordt gedomineerd door enkele grote spelers. Deze spelers hebben de markt per land verdeeld (nationale verkaveling). Om hun markten te beschermen hebben leveranciers hun nationale posities versterkt door proprietary systemen te verkopen. Dit is tot op heden een obstakel voor echte interoperabiliteit.

Universiteiten zijn regelmatig betrokken bij onderzoek naar biometrie, maar moeten vaak de ervaring van het dagelijks werken met biometrie in de praktijk ontberen. Financiering voor technisch georiënteerd onderzoek is in beperkte mate voor handen, waardoor innovaties in de biometriemarkt moeizaam worden gerealiseerd. Dit hangt samen met het feit dat het grootste deel van de markt historisch is bepaald en daar willen de marktleiders het liefst geen verandering in brengen. Daar komt bij dat kleine innovatieve bedrijven maar zelden de kans krijgen om zich op de grote opdrachten te profileren, omdat zij de juiste contacten en omvang ontberen.

Biometrische standaards zijn relatief nieuw en daarom soms onvolledig of onvoldoende geïmplementeerd en/of testbaar. Bepaalde staandaards zijn nog niet gereed, zoals bijvoorbeeld de staandaards met betrekking tot image quality van zowel de gezichtsopname als de vingerafdruk. Zeker in de periode 2000-2005 waren vrijwel alle relevante technische standaards afwezig en bestonden alleen nog maar de eerste aanzetten daartoe.

De belangrijkste duurzame maatregel om een optimale kwaliteit en betrouwbaarheid te verkrijgen is het besteden van alle aandacht aan de processen, procedures en benodigde techniek bij de eerste registratie (i.c. de paspoortaanvraag). Het garanderen van kwaliteit door te verwijzen naar CBEFF, BioAPI of ISO-standaard 19794-4 (of een andere standaard uit diezelfde serie) is onvoldoende. De standaarden die dat wél kunnen, zijn nog in de maak en de komende jaren nog niet toepasbaar.

De industrie is nog sterk gericht op het beschermen van de eigen markt, onder andere door het aanbieden van proprietary producten. Zelfs de implementatie van

het onafhankelijke kwaliteitssysteem NFIQ biedt geen garanties voor uniforme interpretatie van image quality door leveranciers. Interoperabiliteit is daarom nog geen gemeengoed. Het nemen van alle mogelijke maatregelen om de kwaliteit en integriteit van de biometrische data te optimaliseren is de meest voor de hand liggende manier om interoperabiliteit en prestaties te optimaliseren.

'In house testing and benchmarking' door overheden is weliswaar goed voor het begrip van de eigen eisen en de mate waarin een biometrische toepassing die kan invullen, maar vormt een risico voor de onafhankelijkheid, transparantie en uiteindelijk de kwaliteit van de tests, proeven en studies. Een zeer kritische houding ten opzichte van de eigen kennis en onafhankelijkheid, alsmede een open houding ten aanzien van onafhankelijke meningen en afwijkende inzichten kunnen daartoe een tegenwicht bieden.

In het algemeen is er onvoldoende capaciteit en ervaring opgebouwd bij onafhankelijke testlaboratoria. Dat is onder andere het gevolg van 'in house testing and benchmarking' door de overheden. Resultaten van de tests kunnen daarbij makkelijk ten prooi vallen aan tunnelvisie, politieke krachtenvelden en soms zelfs onkunde. Voor buitenstaanders kan het vervolgens bijzonder lastig zijn om een helder beeld te krijgen van de stand van zaken rond de eisen en de te verwachten prestaties van een biometrisch systeem en het succes van een eventuele implementatie.

# DEEL III Politiek en Beleid

# 8. Studies en proeven

## *8.1. Inleiding*

Aanleiding voor de verhandelingen over techniek en markt in de delen I en II van deze studie is de observatie dat in het politieke debat het lijkt alsof partijen niet altijd het besef hebben hoe de biometrische techniek in zijn context begrepen moet worden. Een voorbeeld daarvan is het antwoord op 26 maart 2010 van staatsecretaris Bijleveld op de vragen van Ronald van Raak van de SP. Daarin vraagt hij hoe het staat met de kwaliteit van de vingerafdrukken en eventueel daarmee samenhangende fouten. De vraag en het antwoord luidden als volgt:

Vraag Van Raak:
*"Hoe staat het met de kwaliteit van de afgenomen vingerafdrukken? Is het waar dat deze in sommige gevallen laag is? Worden hierdoor fouten gemaakt? Zo ja, hoe vaak komt dit voor? Wat zijn de mogelijke gevolgen voor de betrokkenen?[29]"*

Antwoord staatssecretaris Bijleveld:
*"De kwaliteit van de vingerafdrukken wordt, conform de specificaties van de Europese Commissie, bepaald aan de hand van de ISO-standaard 19794-4.*
*....*
*De burger kan of bij de uitgifte van het document of daarna in de gemeente waar het reisdocument is aangevraagd vragen om de vingerafdrukken uit te lezen die in de chip van het reisdocument zijn opgeslagen. De twee in de chip opgenomen vingerafdrukken worden dan op een scherm getoond[30]."*

Het eerste antwoord aangaande de kwaliteit is simpelweg niet correct. ISO 19794-4 bepaald niet de kwaliteit van de vingerafdrukken. Dat kunt u nalezen in Deel II van deze studie. Het tweede antwoord toont een diep onbegrip van de technologie: een burger mag en kan nooit in staat worden geacht om zonder speciale scholing en/of training te beoordelen of de vingerafdrukken op een print of een scherm

29 Zie voor deze vragen: http://ikregeer.nl/document/kv-2010Z05459
30 Zie voor deze antwoorden: http://ikregeer.nl/document/ah-62670?format=pdf

daadwerkelijk overeenkomen. Een baliemedewerker kan dat ook niet, maar daar wordt het ook niet van verwacht. En wat als het niet klopt?
Verder geeft Bijleveld geen antwoord op de vraag over de kwaliteit. Wel zegt zij dat vanwege de Europese verordening er ook slechte kwaliteit afdrukken kunnen worden opgeslagen. Zegt ze daarmee dat onze processen en procedures dan ook van slechte kwaliteit mogen zijn en dat we vanuit het oogpunt van het verkrijgen van een optimaal functionerend systeem geen maatstaf hoeven te hebben voor de kwaliteit? Wanneer kunnen we dan spreken van een succesvol biometrisch paspoort? Wat is de norm?

Hoe kan het dat over zo een belangrijk onderwerp, dat letterlijk elke burger raakt, zo weinig kennis is bij diegenen die de besluiten nemen? Hoe komt het dat er vanuit de Tweede Kamer niet direct iemand opstaat en zegt dat de antwoorden niet kloppen noch volledig zijn en dat het huiswerk opnieuw moet?

Door de jaren heen is er veel begripsverwarring ontstaan, waar niemand echt zijn vinger achter kon krijgen. Steeds groter werden de termen en ambities als het ging over het doel dat de biometrie moest dienen: van 'look alike fraude' tot terrorismebestrijding; van verificatie van het paspoort tot identificatie bij rampen; van het beveiligen van het paspoort tot identiteitsfraude in brede zin. Maar de consequenties van deze grote termen voor de uitvoering worden niet consequent uitgewerkt en doorgevoerd, zoals onder andere blijkt uit het bovenvermelde geciteerde vraag & antwoord. Anders zou de burger wél in staat zijn gesteld een automatische verificatie te doen bij ontvangst van zijn paspoort.

In dit hoofdstuk wordt in meer detail gekeken naar hoe de overheid met de techniek is omgegaan. Dat betreft zowel de voorbereidingen van het biometrische paspoort als de huidige implementatie. Er zal enerzijds gekeken worden naar de studies en pilots die er zijn uitgevoerd, anderzijds naar de vertaling daarvan door de overheid richting de politiek. De nadruk zal worden gelegd op de techniek en niet op het parlementaire proces als zodanig. Daarin complementeert voor deze studie de parallelstudie *Happy Landings?* van Vincent Böhre.[31] Echter, vanuit het centrale startpunt van deze studie,

31 Beschikbaar op www.wrr.nl.

de techniek, is het interessant om te kijken naar de invloed die politiek en beleid hebben gehad op de ontwikkeling van de biometrische techniek en de processen en procedures daaromheen. Hierbij is in eerste instantie het kernprobleem als de drijvende factor achter het biometrische paspoort van belang.

### *8.2 Setting the scene*

Als resultaat van het proect NGR (Nieuwe Generatie Reisdocumenten) heeft de Nederlandse overheid in 2001 een nieuw paspoort op de markt gebracht. De ambities waren hoog: men was vastbesloten om af te rekenen met de zogenaamde 'paspoortaffaire', die Nederlandse bestuurders en bewindslieden hardnekkig bleef achtervolgen. Door diverse beveiligingstechnieken (o.a. polymeer houderpagina, 'gaatjes-foto') en het overgaan op centrale personalisatie was de fraude met paspoorten aanzienlijk teruggebracht.[32] In Europa en daarbuiten heeft Nederland daarvoor veel bijval gekregen en liep in elk geval in Europa met deze hightechontwikkelingen in de voorste regionen van de paspoortinnovatie. Omdat men meende dat na deze verbeteringen de fraude zich zou gaan verplaatsen naar 'look alike fraude', ging men al rond 1999 nadenken over de mogelijkheden die biometrie zou kunnen bieden om deze vorm van fraude te kunnen bestrijden. 'Look alike fraude' is in het politieke veld tot zeker 2005 dé drijvende factor geweest voor de introductie van het biometrisch paspoort.

In de beginperiode klonken er naast veel positieve ook reeds kritische geluiden. In 1999 uitte TNO al bedenkingen met betrekking tot de prestaties en veiligheid. Latere studies gaven daar onvoldoende antwoord op. Naast veiligheid en prestaties moest er ook gekeken worden naar standaardisatie, acceptatie van biometrie door burgers en de integratie van de techniek in de bestaande infrastructuur. De standaardisatie was nog maar net gestart. En burgers konden zich maar weinig voorstellen van wat biometrie betekent. Men had er immers geen ervaring mee in het dagelijks leven.

32 Einddocument Regionale Samenwerking Identiteitsfraude, in 2002 opgeleverd door de Projectgroep Regionale Samenwerking Identiteitsfraude bestaande uit vertegenwoordigers van OM, GBA, BPR, Min.SZW, NVVB en Politie.

Het kernprobleem was (en is nog steeds) het tegengaan van 'look alike fraude' en het betrouwbaarder maken van het aanvraag- en uitgifteproces. Nederland was in 1999 al met de gedachtevorming hierover begonnen en in 2004 kwam de Europese Directive EC2252 als wettelijk uitgangspunt. Voor dat doel kwam de vingerafdruk het meest in aanmerking. Echter, vanaf circa 2005 vindt er een omslag plaats en wordt de probleemstelling breder getrokken naar identiteitsfraude in het algemeen in combinatie met bepaalde vormen van opsporing en vervolging. Daarvoor zou centrale opslag van de vingerafdrukken randvoorwaardelijk zijn. Deze omslag roept verschillende vragen op. Ten eerste wat de onderbouwing is voor deze randvoorwaardelijkheid. Ten tweede hoe de technische haalbaarheid is beoordeeld en wat daar de criteria voor waren. Na die omslag zijn er geen technische studies of proeven meer geweest. Wel vindt er in de jaren erna een debat plaats in de Tweede Kamer, zij het met horten en stoten. De Kamer stelt regelmatig vragen over beveiliging, prestaties en privacy en wordt op gezette tijden netjes geïnformeerd. Maar er blijft een gevoel aanwezig dat niet alles duidelijk is. Men heeft moeite met het interpreteren van de antwoorden op aan de overheid gestelde vragen en met het doorgonden van de techniek. Maar alles gaat door en de nieuwe Paspoortwet wordt aangenomen. Hoewel nog niet geheel in werking, wordt in september 2009 begonnen met het afnemen van de vingerafdrukken. De staatssecretaris belooft het proces nauwkeurig te volgen. Maar als uiteindelijk de evaluatie komt, blijkt dat er maar weinig harde feiten in staan.[33] Met name de prestaties en de veiligheid worden nauwelijks inzichtelijk gemaakt op basis van concrete informatie.

Door de tijd heen zijn in het politieke debat verschillende doelstellingen voor de invoering van biometrie de revue gepasseerd. Hier een korte opsomming van de belangrijkste.

- Voorkomen 'look alike fraude'.
- Voorkomen van identiteitsfraude.
- Veiliger maken van het aanvraag- en uitgifteproces.
- Het betrouwbaarder maken van het verificatieproces.
- Identificatie bij rampen.

33 BZK (2005).

- Identiteitsvaststelling van verdachten van strafbare feiten waarvoor voorlopige hechtenis is geëist.
- Faciliteren van geautomatiseerde grenspassage.
- Voorkomen van dubbele identiteiten.
- De-duplicatie.[34]

Daarnaast zijn in het politieke debat uitspraken gedaan die het gebruik van biometrie zouden moeten afbakenen.

- Vissen in de database op basis van uitsluitend de biometrie (1:n) is niet toegestaan.
- De database wordt geen opsporingsregister.
- Zoekaanvraag verloopt uitsluitend via de officier van justitie.

Dit is een nogal uitgebreide lijst met een veelheid aan functies met soms nogal brede begrippen. Het maakt het voor de burger er niet duidelijker op, terwijl die nu juist een helder beeld zou moeten hebben.

Tussen 1999 en 2005 hebben er diverse studies en pilots plaatsgevonden die gezamenlijk ruggesteun hebben moeten verlenen aan de (politieke) besluitvorming rond de nieuwe Paspoortwet en het gebruik van biometrie daarbinnen. In 2005 verscheen het laatste rapport in de reeks: *Evaluatierapport Biometrieproef '2b or not 2b'*. Daarna zijn geen nieuwe (haalbaarheids)studies of proeven meer gedaan. Dat betekent dat men heeft gevonden dat het gebruik van biometrie zoals nu in de Paspoortwet is vastgelegd haalbaar, noodzakelijk en financiëel verantwoord is. In de volgende paragrafen worden de studies en pilots zoveel mogelijk in chronologische volgorde besproken om te zien of daar voldoende onderbouwing voor is geweest.

### *8.3 Quick Scan Biometrie: Alle Mensen Zijn Ongelijk (TNO, 1999)*

Het rapport *Quick Scan Biometrie* is in opdracht van BPR door TNO in 1999 uitgevoerd door beveiligingsexpert Ruud van Renesse met als belangrijkste vraag in

34 De-duplicatie is het detecteren in een database van personen met meerdere identiteiten aan de hand van de biometrische gegevens.

hoeverre biometrie geschikt is als middel ter bestrijding van 'look alike fraude' met identiteitsdocumenten. Dit was nog vóór '9-11' en dus voordat de grote internationale druk bestond rond de bestrijding van terrorisme. De Nederlandse overheid was in die tijd al in een gevorderd stadium met het project NGR (zie paragraaf 8.2), waaruit zoals we weten in 2001 een sterk verbeterd paspoort was voortgekomen. Biometrie leek een antwoord op 'look alike fraude' te zijn, maar veel was nog onbekend. De door de opdrachtgever gegeven scope van de studie was dat:

> *"biometrie in de verificatiemode zal worden toegepast, d.w.z. dat de biometrische procedure de vraag beantwoordt of de aanbieder van het reisdocument de rechtmatige houder ervan is."*[35]

'Verificatiemode' houdt in dat er uitsluitend een 1:1 vergelijking wordt gedaan met de biometrische gegevens in de chip van het paspoort. Centrale opslag en de daarmee samenhangende 1:n zoekacties vallen er dus buiten.

Enkele van de conclusies van het rapport zijn de volgende.

- *De foutpercentages FRR, FAR en FTE zijn van cruciaal belang voor het functioneren van een biometrisch systeem. Een specificatie van vereiste foutpercentages zal afhangen van het vereiste niveau van beveiliging (toelaatbaar percentage succesvol bedrog) zowel als van het toelaatbaar aantal ten onrechte afwijzingen.*
- *Daar biometrie niet foutloos functioneert, dient - ongeacht de biometrische toepassing - in adequate 'fall-back' procedures te zijn voorzien. De 'fall-back' procedure dient daarom instrumenten te bieden die een nauwkeurige scheiding tussen de beide vormen van afwijzing mogelijk maken. Indien zulke instrumenten niet (kunnen) worden geboden, wordt het goede functioneren van het biometrische systeem ondergraven en heeft de toepassing ervan geen zin.Teneinde adequaat te kunnen zijn, dient een 'fall-back' procedure de bevoegdheid in te houden tot een identiteitsonderzoek.*
- *Het is onverstandig over te gaan tot landelijke invoering voordat aan alle randvoorwaarden is voldaan. Wanneer de invoering vroegtijdig en*

35 TNO (1999).

*onvoldoende voorbereid plaatsvindt en daardoor mislukt, is de kans waarschijnlijk verkeken de fout binnen afzienbare tijd te herstellen.*

- *De noodzakelijkheid dient door de gebruiker te worden ingezien. Een goede communicatie naar de gebruiker is daarom van groot belang. Duidelijk dient te worden uitgelegd waarom biometrie noodzakelijk is, wat de voordelen zijn voor de gebruiker, dat de gegevens niet in een centrale database zullen worden opgeslagen en niet door de politie kunnen worden gebruikt.*[36]

In bovenstaande conclusies zijn duidelijk kritische succesfactoren te onderscheiden. Er wordt verwezen naar een 'vereist niveau van beveiliging', een eerste – en misschien wel de laatste – poging in de reeks onderzoeken die nog zouden worden verricht, om te komen tot een norm voor de prestaties van het biometrische systeem. Dat vereiste niveau zou het uitgangspunt moeten zijn voor de specificatie van de toelaatbare foutpercentages. Deze percentages zouden vervolgens het uitgangspunt voor de haalbaarheidsstudies en proeven moeten zijn. Van belang is verder de opmerking, waarin impliciet wordt gesteld dat bij de registratie van de biometrische gegevens er een zeer goede controle moet zijn op de integriteit en authenticiteit van de biometrische en andere persoonsgegevens. Omdat dat controleproces ter plaatse en direct plaatsvindt, stelt dat hoge eisen aan het baliepersoneel en aan de technische mogelijkheden om deze gegevens direct te kunnen verifiëren en te controleren. TNO stelt in het rapport dat bij afwezigheid van deze controles de kans op fraude groot is en het systeem dan zinloos is.

Relevant zijn ook de opmerkingen die TNO plaatst met betrekking tot de zogenaamde 'fall back'-procedures. Dat zijn procedures die in werking gaan wanneer er geen herkenning plaatsvindt. De vraag is dan namelijk of deze niet-herkenning (of non-match) terecht was of niet.

> *"Waar in het geheel geen 'fall-back' procedure bestaat, zal zelfs iedere afwijzing door de biometrische apparatuur leiden tot een weigering van de gevraagde dienst, uiteraard in veel gevallen of zelfs in vrijwel alle gevallen ten onrechte. Met andere woorden, een brede toepassing van biometrie om identiteitsfraude te bestrijden heeft slechts zin wanneer deze toepassing gepaard gaat met*

36 Idem.

*adequate 'fall-back' procedures. Teneinde adequaat te kunnen zijn, dient een 'fall-back' procedure de bevoegdheid in te houden tot een identiteitsonderzoek.[37]"*

De kritische aantekeningen uit dit rapport zullen tot op de dag van vandaag door experts worden onderschreven. Desondanks leek de opdrachtgever er niet blij mee te zijn. Ruud van Munster, biometrieexpert bij TNO, zegt over de 'Quick Scan Biometrie' het volgende:

*"Het rapport werd door BPR gearchiveerd en pas later bekendgemaakt. (...) Het rapport was tamelijk kritisch over het gebruik van biometrie; dit echter ook in het licht van het feit dat de overheid nog geen heldere doelen voor biometrie had aangegeven. Het rapport ging over biometrie in het paspoort voor grenspassage, gebruik van biometrie in het gemeentehuis en thuisgebruik. (...) Zelf vond ik het rapport nog relatief mild, maar toch reageerde BPR als door een wesp gestoken.(...) Het was voor TNO vervolgens lastig om opdrachten van de overheid op biometriegebied te krijgen. [...] BPR wilde TNO echter alleen nog bij dit project betrekken [auteur: i.e. het onderzoek 'Biometrics Against Look Alike Fraud in the Next Genreation Travel Documents'] als Ruud van Renesse uit het projectteam zou worden teruggetrokken.[38]"*

### *8.4 Pilots in 2000-2002*

In de periode 2000-2002 zijn onder leiding van BPR diverse pilots voorbereid en uitgevoerd. Inmiddels was het duidelijk dat biometrie een rol toebedeeld zou krijgen bij de bestrijding van 'look alike fraude' en dat de ICAO bezig was met het toewerken naar een wereldwijde standaard. Hoewel de pilots maar weinig aansluiting hadden met de plannen van de overheid rond het biometrische paspoort en de ontwikkelingen bij de ICAO, worden ze voor de volledigheid hieronder toch kort besproken.

Op 11 december 2000 startte een pilot met circa 50 gebruikers in Delft met als titel 'Loketaanhuis.nl'. De toepassing was het bieden van elektronische dienstverlening via internet door verschillende dienstenleveranciers in de sociale zekerheidsector. Er werd een smartcard gebruikt die door de vingerafdruk werd beveiligd. Een smartcard reader

37 Idem.
38 WRR-interview, Den Haag 16 februari 2010.

was verbonden met een pc. De beknopte rapportage van BPR noemt geen cijfers over de prestaties van de biometrische verificatie.

In Rotterdam startte een 6 maanden durende pilot van juli t/m december 2001. De pilot maakte het de vreemdelingen in Rotterdam mogelijk op elektronische wijze te voldoen aan hun maandelijkse meldingsplicht. Hiervoor stond er in de hal van het kantoor van de Vreemdelingendienst een meldzuil. Deelname aan de pilot geschiedde geheel op vrijwillige basis. die zich maandelijks bij de vreemdelingenpolitie moesten melden. Het doel was het vergroten van de service richting de vreemdelingen (geen afspraken meer nodig) en tegelijkertijd het beter stroomlijnen van het meldingsproces op het kantoor van de politie. Er werd een contactloze chip gebruikt (zoals beoogd voor het toekomstige paspoort). De twee irissen van de vreemdeling werden in een digitale code opgeslagen op de chip. Het meldingsproces vond plaats aan een onbemande kiosk. Een van de twee irissen van de vreemdeling werd vergeleken met de data in de chip. Daarmee werd geverifiëerd of de persoon die zich meldde ook daadwerkelijk bij de kaart hoorde.[39]

Een derde pilot vond plaats in Amsterdam-Zuid en betrof het zogenaamde 'electronische loket'. In de pilot Amsterdam-Oud Zuid beproefde BZK een elektronische identiteitskaart waarmee de deelnemers aan de pilot zich elektronisch konden identificeren. De elektronische identiteitskaart was voorzien van een zogenaamde elektronische handtekening en een template met een vingerafdruk voor verificatie van de identiteit van de deelnemer. Verder was in opdracht van het ministerie een elektronisch proces ontwikkeld waarmee de pilotdeelnemer elektronisch zijn/haar mening kon geven over voorstellen van het stadsdeel Oud Zuid met betrekking tot de inrichting van de wijk. Via het internetadres www.Stadionline.nl (open/publiek gedeelte van de site) kon er met behulp van de elektronische identiteitskaart ingelogd worden op het besloten gedeelte van de site.[40]

Een beknopte rapportage van alle drie hierboven beschreven proeven is te vinden in de bijlage van van de brief van de minister aan de Kamer dd 19 december 2003 (kenmerk BPR2003/U87221). De rapportage meldt alleen voor de laatste proef een Failure To

39 *Kleinschalige Pilots*, BPR. Beschikbaar als bijlage bij Brief van 19 december 2003, Kenmerk BPR2003/U87221
40 Idem.

Enroll (FTE) van 5%. De oorzaak wordt niet besproken. Voor geen van de drie gebruikte systemen worden de FRR of FAR vemeld. Wel vinden we een melding van een percentage van 6% voor de FRR in de paper van Ruud van Renesse *Implications of Biometrics for Travel Documents*, die hij had geschreven ten behoeve van het 5th International Conference on Fraudulent Documents, Amsterdam 11 april 2002 (lees verderop in deze paragraaf meer over deze paper). Overigens is deze paper uiteindelijk niet door de organisatoren van de conferentie gepubliceerd.

In 2002 begon Lies de Leeuw[41] haar dienstverband bij Agentschap BPR in de functie van Senior Projectleider Innovatieprojecten. Hoewel zij niet betrokken was bij de opzet en uitvoering van de pilots, had zij wel te maken met de resultaten ervan. Zij zegt daarover het volgende.

> *"[…] De veiligheid van het verhaal daar was ontzettend laag ingezet vanuit de gedachte dat het karretje moest rollen. Het moest blijken dat alles 'het doet'. Dat alle kleppen open stonden werd niet als relevant gezien. Het was meer zo: "werkt het?". Zo van: als ik op dit knopje druk, gaat dan dat lampje branden? De security is lichtgewicht afgehandeld en dat is dan nog zachtjes uitgedrukt; het was een rommeltje. Security leek geen eis te zijn of in ieder geval iets dat niet de moeite waard was om in ontwerp en test mee te nemen. Er werd erg gekeken naar theoretische performance cijfers geclaimd door de leverancier. Zoals bekend liggen de performance indicators van leveranciers altijd hoger dan de performance zoals die in onafhankelijke laboratoria wordt vastgesteld. Maar je had allerlei redenen om aan te nemen dat het in de praktijk anders was. Ten eerste omdat een leverancier altijd zijn spullen oppoetst alvorens hij ze in de etalage zet. Maar ten tweede – ook al zou de leverancier super eerlijk zijn - dan nog is er een groot verschil of het werkt bij een gebruikersgroep van pakweg 100 personen danwel bij een groep zo groot als een complete bevolking met allerlei wisselende omgevingen en overige factoren die erbij komen kijken (omgevingsfactoren en diversiteit van doelgroep in termen van ras, sexe, persoonlijke omstandigheden, handicaps). Alle in de periode 2000-2002 gedane proeven (o.a. Pilot Rotterdam, Kiezen op Afstand)*

41 Elisabeth (Lies) de Leeuw heeft een Master of Security and Information Technology (MSIT) en is adviseur Beveiliging en Identiteitsmanagement. In oktober 2004 publiceerde zij haar thesis *Risks and Threats of Biometric Technology in Nationional Identity Management*, te downloaden via www.pvib.nl/scripties. Zij ontving daarvoor de Joop Bautz Information Security Award (www.jbisa.nl). Deze award is in 2001 in het leven geroepen door de verenigingen GvIB, PI, ISACA, ITSMF, NGI, NOREA en VBN.

*zijn veel te kleinschalig geweest en hadden het gehalte van probeersels. Bovendien klopte de scenario's niet: de Pilot Rotterdam maakte gebruik van de iris en voorzag in een service en was bovendien gericht op een specifieke doelgroep (vreemdelingen van buiten de EU), Kiezen op afstand was een thuis-situatie en voorzag ook in het leveren van een dienst. Dit is allemaal niet van toepassing op het paspoort. Het ging vooral over FRR vanwege de impact daarvan op de doorstroming. Dat is wel belangrijk, maar niet het primaire doel voor het toevoegen van biometrie aan de reisdocumenten. Dat is namelijk de FAR. En daar wil niemand echt naar kijken. Dat is toch wel typisch want dat is toch in feite waar het allemaal om is begonnen. FAR is echter moeilijk vast te stellen want het betreft een ´open´ groep. Maar juist voor de FAR is het belangrijk om dat wel ´levensecht´ te testen omdat je dan ook de gekheden van alledag plus de pogingen tot fraude bij de hand hebt. Maar misschien kunnen we iets met fraude simulatoren in het lab? In ieder geval is dat nooit geprobeerd."* [42]

Lies de Leeuw staat niet alleen in haar observatie. Ruud van Renesse zegt in zijn paper ter uitreiking tijdens de onder de auspiciën van Interpol georganiseerde 5th International Conference on Fraudulent Travel Documents te Amsterdam over deze pilots het volgende.

*"The question may arise what the relevance of such small scale pilots is for the detection of 'look alike' applications. The pilots invariably involve user services and thus involve cooperative participants. However useful the results of such pilots may be, they are if little to no value to assess the prospect of a nationwide application biometrics to travel documents in order to solve the 'look alike' problem."*[43]

In andere woorden: volgens Van Renesse kunnen aan de hand van de pilots geen conclusies worden getrokken over de toepasbaarheid van biometrie ter bestrijding van 'look alike fraude' met paspoorten en andere id-documenten. Afgezien van zijn opmerkingen over de pilots zegt hij ten aanzien van de veiligheid van biometrie het volgende.

42 WRR-interview 1april 2010.
43 Van Renesse (2002).

*"This paper recognizes some inherent problems: 1) due to human factors, false reject rates will expectedly be considerable, and look-alikes will claim to be falsly rejected, 2) the look-alike may sabotage the biometric functionality of the traveldocument and 3) the enrolment proces may be fraudulently frustrated."*[44]

De paper van Renesse gaat onder andere in op de mogelijkheden om het biometrische systeem te sabboteren, zowel bij de registratie als bij de verificatie. Daarnaast voorspelt hij een FRR van zeker tussen 1% en 5% als gevolg van niet optimale omgevingsomstandigheden en onervarenheid van de te registreren persoon met biometrische apparatuur. Van Renesse constateert verder dat het voor baliemedewerkers eigenlijk niet goed mogelijk is om onderscheid te maken tussen een terechte reject of een onterechte. Oftwel: het is moeilijk het verschil te meten tussen de True Reject Rate (TRR) en de False Reject Rate (FRR). Dit heeft consequenties voor het veiligheidsniveau van het aanvraagproces en voor de evalueerbaarheid van de veiligheid van het systeem. Voor baliemedewerkers is het moeilijk om de juiste vervolgactie te bepalen na een reject. Voor een uitvoerige controle ter plaatse is immers te weinig tijd en expertise. Bovendien kunnen er irritaties ontstaan bij de paspoortaanvrager. Om het aantal false rejects te reduceren lijkt de meest voordehandliggende oplossing het omlaag brengen van de drempelwaarden. Maar daardoor worden er ook meer slechte kwaliteit afdrukken toegelaten met alle gevolgen voor de prestaties van het systeem als geheel (zie Deel I Techniek en proces). Eenzelfde redenering geldt voor de acceptatie: het is moeilijk om te bepalen of een acceptatie terecht is (True Accept) dan wel onterecht (False Accept). Bij registratie- en controlepunten levert dit volgens Van Renesse belangrijke problemen op met betrekking tot de veilgheid. Om de veiligheid van een biometrisch systeem goed te kunnen beoordelen is het van belang om in de praktijk van de toepassing de TAR en FAR goed te doorgronden. Van Renesse geeft in zijn paper een aanzet tot het specificeren van veiligheidseisen van een biometrisch systeem. We zullen zien dat deze aanzet geen vervolg heeft gekregen.

44 Idem.

### *8.5 Verkennend Onderzoek Biometrie (Veldkamp, jan. 2003)*

Dit onderzoek is uitgevoerd door bureau Veldkamp en bestaat uit een kwantitatieve fase (concept afgerond in november 2002) een kwalitatieve fase (afgerond en gepresenteerd in de definitieve eindversie in januari 2003). De opdracht luidde:

> *"Het uitvoeren van een onderzoek naar de kennis en houding van de burger ten opzichte van biometrie in reisdocumenten, uitgevoerd in opdracht van de Rijksvoorlichtingsdienst/Publiek en Communicatie ten behoeve van het ministerie van Binnenalndse Zaken en Koninkrijksrelaties, Basisadministratie Persoonsgegevens en Reisdocumenten (BZK/BPR)."*[45]

Het meest relevante voor de waarde van een dergelijk onderzoek is het kennisniveau van het ondervraagde publiek. Immers, wanneer men weinig kennis en achtergondinformatie heeft van biometrie en de toepassingsmogelijkheden, zijn de meningen daarover minder betrouwbaar. Bij het doorlezen van de samenvatting valt direct op dat de eerste onderzoeksvraag, namelijk het bepalen van het kennisniveau van het brede publiek ten aanzien van biometrie, niet duidelijk wordt beantwoord. Toch komen we bij het doorlezen van het gehele rapport aan het begin van het kwalitatieve gedeelte in paragraaf 2.2 (p. 47) een duidelijke conclusie tegen.

> *"Het begrip biometrie roept allerlei associaties op, maar vrijwel geen enkele associatie klopt. Slechts een enkeling legt een verband met irisscans of vingerafdrukken, maar deze vormt de uitzondering op de regel. Het begrip zelf behoeft dus heel wat uitleg en is zeker zonder context voor vrijwel iedereen een raadsel."* [46]

De eerste vraag van de onderzoeksopdracht over het kennisniveau van de burger ten aanzien van biometrie wordt in het rapport dus vrij duidelijk beantwoord: mensen hebben geen idee waar biometrie precies over gaat. Deze conclusie vinden we niet terug in de samenvatting.

45 Veldkamp (2003).
46 Idem.

In het kwalitatieve deel wordt vervolgens gezegd dat *"na enige tekst en uitleg men in het algemeen geen moeite heeft met een dergelijke techniek. Sterker nog: men ziet het als een prima middel om fraude te voorkomen".*[47] Maar als men verder leest blijkt eveneens dat na enige discussie de groep van respondenten wel degelijk tot een hele opsomming van nadelen en risico's komt en dus gaandeweg kritischer wordt. Respondenten komen dan met opmerkingen als "je kunt je afvragen of alles wat er bij de overheid ligt, zo goed gebeurt" en "het is mensenwerk, een mens laat zich verleiden".
Er lijkt sprake te zijn van een toenemende scepsis als gevolg van voortschrijdend inzicht. Dit heeft bij het kwantitatieve onderzoek ontbroken, omdat daarvoor een vragenlijst werd gebruikt zonder discussie of overleg.
Andersom zou het betekenen dat mensen positiever zijn over de toepassing van biometrie naarmate ze er minder van weten. Als je dat combineert met de conclusie dat de meesten in eerste instantie niet veel van biometrie begrijpen, wordt de belangrijkste uitkomst van het kwantitatieve deel bevestigd: namelijk dat het overgrote deel van de respondenten een positieve houding heeft. Echter, gezien het gebrek aan kennis is die conclusie niet zonder meer bruikbaar om daarmee in het algemeen aan te tonen dat de burgers het gebruik van biometrie in meerderheid toejuichen. Bovendien, omdat in de tijd de doelstellingen zijn veranderd (nl. van lokale opslag van de biometrische gegevens naar centrale opslag), kan dit onderzoek als verouderd en niet meer relevant worden beschouwd.

### *8.6 Technical Survey (2002)*

*Biometrics Against Look Alike Fraud in the Next Generation Travel Documents* – a Technical Survey (VKA/TNO, versie 1.2 Final, 10 dec.2002) is door VKA en TNO als onderaanemer in opdracht van Agentschap BPR uitgevoerd. Het onderzoek vond plaats in het kader van de toepassing van biometrische kenmerken in Nederlandse reisdocumenten. De studie heeft zich beperkt tot publieke verkrijgbare documenten. Ook zijn er niet-publieke documenten geraadpleegd die door het ministerie van BZK[voluit] voor deze survey ter beschikking waren gesteld. Er zijn alleen documenten in beschouwing genomen die in het Nederlands, Engels of Duits waren geschreven. Omdat het doel van de biometrie uitsluitend de bestrijding van 'look alike fraude' was, is er bij

47 Idem.

het vergelijken van de prestaties van biometrische producten alleen gekeken naar 1:1 verificatie. Vanwege de ICAO-richtlijn zijn alleen gezicht, vinger en iris in beschouwing genomen. Daarnaast is ook gekozen zich te beperken tot een enkele use case: het toepassen van biometrie in gecontroleerde omgevingen met direct toezicht voor tweedelijnsverificatie. Dat betekent dat de biometrie alleen maar gebruikt wordt in aanwezigheid van een beveiligingsambtenaar, die controleert op fraude zoals siliconenvingers, bewerkte contactlenzen, valse baarden enzovoorts. Door deze beperkingen zo expliciet aan te brengen laten de auteurs weten dat zij beseffen wat het uiteindelijke doel is dat de overheid (althans toen) voor ogen had, en wat de risico's van biometrie zijn ten aanzien van de veiligheid.

De onderzoeksvragen voor deze studie waren als volgt:

1. *collect experience data*
    a. *collect experience facts on usage of biometrics for the anticipated application area and on the anticipated large scale*
    b. *judge the technical effects of up-scaling a pilot-project to a large scale operational implementation*
    c. *assess how the performance of biometrics techniques in practice relates to those of pilot and laboratory situations*
    d. *based on the previous question: judge the value and sense of reality of the performance indicators as quoted by suppliers*
2. *collect and merge data of recent and independent tests*
    a. *collect data of recent and independent tests and comparisons of biometric techniques. Source documents may be obtained through BPR*
    b. *merge data of different tests to obtain an objective and balanced view*
    c. *judge to what extent tests and researchers indicate the applicability of biometrics. Take into account the anticipated application area, the anticipated scale, the expected user profile and the relevant techniques.*[48]

De studie kijkt met een realistische blik naar de technologie. Hieronder volgen enkele van de belangrijkste bevindingen.

48 VKA/TNO (2002).

De eerste algemene conclusie is dat er weliswaar veel bestaande studies beschikbaar zijn, maar dat deze vrijwel geen kwantitatieve informatie bevatten over de prestaties van de biometrische systemen. Een belangrijke reden daarvoor is dat die informatie veelal vetrouwelijk is. Als gevolg zijn de conclusies van het rapport voornamelijk gebaseerd op testdata van laboratoria, met de aantekening dat het aantal onafhankelijke tests met betrekking tot de prestaties van biometrische verificatiesystemen zeer beperkt is.

In het rapport wordt erkend dat de prestaties van een biometrisch systeem in sterke mate worden beïnvloed door diverse factoren, anders dan de technologie zelf. Bij de totstandkoming van de gegevens waren deze niet meegenomen. In dat licht moeten de in het rapport genoemde cijfers als theoretisch worden gezien. Omdat de invloed van deze factoren (zoals leeftijd, omgevingsfactoren etc.) op de prestaties volgens het rapport onbekend is, heeft dat tot gevolg dat:
a) er geen betrouwbare schattingen gedaan kunnen worden van de te verwachten Failure To Enrol Rate (FTE) voor de in beschouwing genomen toepassing, en
b) het onmogelijk is om met een redelijke mate van betrouwbaarheid na te gaan wat de prestaties van de verificatie zullen zijn (FRR en FAR) voor geen van de drie onderzochte technolgieën (gezicht, vinger, iris) in de beoogde toepassing.

Het is dan ook niet verbazend dat de belangrijkste aanbeveling van het rapport is dat er meer tests, pilots en studies gedaan moeten worden. Het rapport doet daarvoor de volgende aanbevelingen:

> *Preferably, the study should be designed to clarify the effects on:*
>
> - *nation wide population coverage*
> - *template ageing*
> - *look-alikes and "lambs"*[49]
> - *acquisition conditions*
>
> *Since the total error rate generated by a verification system depends on the use case,*

49 Iemand claimt de identiteit van een ander. Hij hoopt op een False Acceptance. Wanneer hij toch wordt geweigerd claimt hij dat hij slachtoffer is van een false rejection door het systeem.

- *a carefull scenario evaluation is recommended*
- *verification systems with adjustable threshold setting are preferred*

*Fall back scenarios are recommended for:*

- *instances of rejection, and for*
- *imposters claiming the identity of a "lamb"; in this case, even imposters that do not resemble the lamb's appearance might, appealing to a succesfull match by the verification system, eventually pass the ID check*

*When an operational verification system has been fully deployed, it is recommended to perform routine operational evaluation, in order to keep track of system performance and of possible changes in operating conditions.*[50]

Belangrijk is dat TNO het belang aangeeft van een strikte afbakening van de use case, om van daaruit de problematiek, technologie en processen in kaart te brengen. Van daaruit kunnen zaken vastgesteld worden zoals de verwachte en reële prestaties en de maatregelen die getroffen moeten worden in de volle breedte om binnen de gegeven use case de gewenste prestaties te verkrijgen.

In de paragrafen hierna zullen we zien in hoeverre de aanbevelingen vorm hebben gekregen in de voortgang van het project.

### *8.7 Project Biometrie Agentschap BPR, 6 juni 2003*

Op 6 juni 2003 verschijnt het rapport *Onderzoek naar de toepassing van biometrische kenmerken voor Nederlandse reisdocumenten*, Den Haag, Project Biometrie, Agentschap BPR. Bevindingen van eerdere studies zoals *Quick Scan Biometrie* uit 1999 en de *Technical Survey* uit 2002 hebben als input gefungeerd.

Het rapport *Onderzoek naar de toepassing van biometrische kenmerken voor Nederlandse reisdocumenten* is definitief vastgesteld op 6 juni 2003 en is als een

50 VKA/TNO (2002).

geconsolideerde versie van diverse deelrapporten op 19 december 2003 in een bijlage van een brief van de minister van BV&K aan de Tweede Kamer gestuurd.

De vraagstelling voor het onderzoek was als volgt.

> *"Zijn de momenteel beschikbare biometrische technologieën geschikt ter bestrijding van 'look alike fraude' en zo ja, welke technologieën verdienen in relatie tot deze doelstelling de voorkeur?*
> *Hoe dient biometrie in de tijd ingevoerd te worden, hierbij rekening houdend met de nationale en internationale context?"*[51]

Een beperking die voor het onderzoek wordt aangebracht is dat verificatie aan de hand van het biometrische kenmerk uitsluitend in fysieke aanwezigheid van de houder van het document en van de verifiërende persoon kan plaatsvinden. Uitsluitend is de verificatie onderzocht die plaatsvindt in een een-op-eensituatie, waarbij het afgenomen biometrisch kenmerk wordt vergeleken met het in het reisdocument opgeslagen kenmerk. Dit is in lijn met het gebruik dat de Europese richtlijn EC2252/2004 ondersteunt. Dat houdt in dat 1:n identificatie niet is onderzocht.

In de uitwerking van de vraagstelling staat met betrekking tot de techniek onder andere dat betrouwbaarheid en toepasbaarheid de belangrijkste uitgangspunten vormen. Betrouwbaarheid wordt niet nader gespecificeerd. Vanwege het karakter van de beoogde toepassing kunnen we aannemen dat daar onder andere de veiligheid van de biometrische technologie onder valt. Dat wil zeggen dat bepaalt dient te worden in hoeverre we zeker kunnen weten dat een Reject een True dan wel een False Reject is, en andersom: of een Accept een True dan wel een False Accept is. Als die gegevens bekend zijn, kun je een uitspraak over de betrouwbaarheid doen. Of het dan geschikt is voor een bepaalde toepassing hangt af van de normen die daarvoor gesteld zijn.

In paragraaf 2.3.1 van het rapport staat overigens ten onrechte dat de FRR en de FAR performance criteria zijn. Het zijn namelijk meeteenheden voor de performance. Criteria worden door de eindgebruiker bepaald. Een meter is geen criterium, maar een afstand. Een meter wordt pas een criterium als iets een meter lang of hoog moet zijn. Dit lijkt

51 BPR (2003).

onschuldig, maar is wezenlijker dan men op het eerste oog zou verwachten. Immers, de fabrikanten drukken de prestaties van hun apparatuur uit in de FRR en FAR. Een niet ingewijde lezer zou dus kunnen denken dat de in tabel 2 genoemde 'performance rates' criteria zijn voor het beoogde systeem. Dat is uiteraard niet het geval. Daarom moeten we concluderen dat de paragraaf over performancecriteria dus feitelijk leeg is, en dat de vraag naar de geschiktheid met betrekking tot de performance dus eigenlijk niet is beantwoord. Omdat betrouwbaarheid en praktische geschiktheid niet onafhankelijk van elkaar kunnen worden beoordeeld (zie ook paragraaf 1.11 en 1.12 van Deel I), is een uitspraak over praktische geschiktheid zonder een norm voor de betrouwbaarheid dus moeilijk te verantwoorden. Een uitzondering kan zijn wanneer men zoveel ervaring heeft met een bepaalde toepassing en techniek in een bepaalde context dat een inschatting van de geschiktheid van technieken met enige betrouwbaarheid kan worden gedaan. Echter, die ervaring was niet aanwezig, hetgeen eerder was geconstateerd in de *Technical Survey* (zie paragraaf 8.6).

Het criterium voor de geschiktheid voor de beoogde toepassing ontbreekt dus. Omdat dit rapport als achtergrondinformatie heeft gediend voor de besluitvorming in de Kamer is dat enigszins verontrustend. Helaas zien we ook geen duidelijke pogingen om tot verantwoorde criteria te komen. Het rapport straalt uit: de techniek werkt, nu alleen nog even testen in de praktijk om de laatste praktische details op te lossen. Het rapport *Quick Scan Biometrie: Alle Mensen zijn Ongelijk* van TNO heeft wel een aanzet gegeven tot het definiëren van criteria, door onder andere zorgvuldig in te gaan op de veiligheidsaspecten en risico's van biometrie in een operationele omgeving. In de hier besproken rapportage vinden we daar nauwelijks een voortzetting van, hetgeen kan leiden tot een rooskleuriger beeld van de mogelijkheden dan de werkelijkheid toelaat. Uiteraard kunnen wel bepaalde praktische criteria in eerste instantie worden uitgesproken, hoewel ook schijnbaar triviale zaken zoals het fysieke formaat van de sensor op zichzelf grote consequenties kan hebben voor andere criteria, zoals betrouwbaarheid. Ander voorbeeld: als een baliemedewerker achter glas moet zitten (zoals op vele consulaten in het buitenland), dan heeft dat grote consequenties in de mate waarin de aanvrager begeleid kan worden bij de afname van de biometrische gegevens. Gebrek aan begeleiding kan leiden tot slechtere afname en dus tot slechtere prestaties van het systeem. Slechtere prestaties leiden tot wachtrijen en een lagere

betrouwbaarheid. Dus als een glazen tussenwand een eis is, zal er genoegen moeten worden genomen met lagere prestaties, óf er moeten maatregelen getroffen worden om het nadeel van deze eis te compenseren.

Met dit rapport *Onderzoek naar de toepassing van biometrische kenmerken voor Nederlandse reisdocumenten* lijkt het pad tot heldere criteria, ingezet door TNO in 1999, te stoppen. Er wordt in de aanbevelingen al gesproken over een praktijkproef waarbij de effecten voor uitgevende instanties en burgers moeten worden getoetst, als ware het aangetoond dat de gekozen biometrische techniek geschikt zou zijn. En ook al zou de techniek zelf in beginsel geschikt zijn (en dat is uiteraard niet uitgesloten), dan nog zal de wijze waarop de techniek wordt ingezet ook geschikt moeten zijn.

De conclusie op pagina 39, dat "het integreren van de hierboven genoemde biometrische technieken in het bestaande aanvraagproces en de huidige infrastructuur goed mogelijk is", is in het licht van het bovenstaande een zwak onderbouwde bewering, omdat duidelijke normen en beoordelingscriteria ontbreken.

Overigens is er wel een (globaal) criterium voor de kosten bepaald. Hierover staat op pagina 40 het volgende.

> "*Deze praktijkproef biedt de mogelijkheid om, met een beperkte inzet van financiële middelen, de alternatieve technische oplossingen bij de uitgevende instanties zodanig te beproeven dat een eventuele landelijke uitrol van biometrie probleemloos kan verlopen.*"[52].

Behalve dat het niet duidelijk is welke alternatieven er precies worden bedoeld, is het gebruik van het woord 'oplossingen' interessant gekozen. Men had ook over 'testopstellingen' of 'proefopstellingen' kunnen spreken. Juist het woord 'oplossingen' wekt de indruk dat het traject van het stellen van criteria, het toesten van de haalbaarheid op basis van die criteria en het formuleren van een helder programma van eisen allemaal achter de rug is. Dit woordgebruik kennen we van de industrie, die daarmee de klant het comfortabele gevoel wil geven dat hij binnenkort alleen nog maar op de startknop hoeft te drukken. In de marketing en sales is dat een techniek om koopintenties te stimuleren en de klant in een positieve richting te manipuleren. Want

welke klant wil nu niet dat al zijn problemen als min of meer opgelost kunnen worden beschouwd?

Tot slot nog enige opmerkingen over de inhoud van paragrafen 5.2, 5.3 en 5.5 over de acceptatie van burgers en privacyaspecten, alsmede over de conclusie op pagina 39, dat "uit publieksonderzoek kan worden geconcludeerd dat de grondhouding van de burger ten opzichte van biometrie overwegend positief te noemen is". Voor een analyse van de grondslag van deze beweringen verwijs ik naar paragraaf 8.5 van deze studie, waar de deelstudie *Verkennend Onderzoek Biometrie* (Veldkamp, jan. 2003) wordt besproken. Hier volstaat de opmerking dat het onderzoek heeft aangetoond dat burgers in meerderheid zeer weinig weten van biometrie.

Aan het in deze paragraaf besproken rapport hebben diverse deelstudies ten grondslag gelegen. Een daarvan is de *Eindrapportage deelstudie techniek*, onderdeel van *Onderzoek naar toepassing van biometrische techniek in Nederlandse Reisdocumenten*. Deze studie kent twee versies: versie 0.91 van 30 mei 2003 en versie 1.1 DEFINITIEF van 29 augustus 2003. De laatstgenoemde versie dateert van een paar maanden na het in deze paragraaf besproken onderzoek. Lies de Leeuw, toen binnen Agentschap BPR verantwoordelijk voor de oplevering van de *Eindrapportage deelstudie Techniek* versie 0.91 zegt hierover het volgende.

*"Mijn bedoeling was dat mijn kanttekeningen bij de technische studie van Klooster & Verdonck + TNO (feb.2003) (onder de kop ´leemtes´) integraal in de tekst zouden worden opgenomen, of, beter nog, in de managementsamenvatting en in de conclusie op hoofdpunten zouden worden samengevat.*

> *"Leemtes:*
>
> 1. *Er zijn onvoldoende ervaringsgegevens over het gebruik biometrie voor de voorziene toepassingsgebieden en de voorziene grote schaal.*
> 2. *Onafhankelijke tests en vergelijkingen van biometrische technieken zijn beperkt voor handen, vaak niet meer actueel en vaak niet geënt op de voorziene toepassingsgebieden.*

3. *er zijn geen ervaringsgegevens over de wijze waarop fraudeurs bij enrolment of verificatie de beoogde toepassing van biometrie trachten te omzeilen.*
4. *het is onbekend aan welke eisen een biometrisch systeem minimaal moet voldoen om 'look alike ' fraude in voldoende cq gewenste mate te bestrijden."*
5. *er zijn geen gegevens voorhanden over hoe in technische zin om te gaan met sabotage van de chip waar ook de biometrische template is vastgelegd.*
6. *het is niet bewezen dat het niet mogelijk is om dmv reverse engineering een biometrisch template te reconstrueren tot een beeld van het oorspronkelijke biometrische kenmerk*
7. *de mate waarin Privacy Enhancing Technologies nuttig cq geschikt zijn voor toepassing op biometrische systemen is onbekend*
8. *de kosten van implementatie en gebruik van biometrische techniek in reisdocumenten zijn niet bekend (studie gaat alleen in op aan te schaffen sw en hw)*
9. *Het is niet bekend of meerdere (verschillende) biometrische templates op 1 chip samengebracht kunnen worden.*
10. *Het is slechts in beperkte mate duidelijk welke keuzes ten aanzien van internationale standaards voor biometrie gemaakt zullen worden, en de mate waarin de keuze voor Nederlandse reisdocumenten hierdoor beperkt kan worden.*

*De bovenstaande punten uit paragraaf 5.5 Leemtes uit versie 0.91 zijn in de definitieve versie1.1 verschoven naar punten onder paragraaf 6 Beantwoording Onderzoeksvragen. Ze zijn omgezet in ambtelijk taalgebruik op een zodanige wijze dat de informatie wordt gekneed en de lezer wordt gemasseerd. Het zijn geen antwoorden op onderzoeksvragen. De titel van de paragraaf verhult de strekking en relevantie."*[52]

52 WRR-interview 1 april 2010.

### *8.8 DRIVeS (2004)*

Op 20 oktober 2004 verschijnt er een rapportage van de hand van Fons Knopjes en Ineke Ruiter, aanvankelijk in dienst bij BPR, maar toen inmiddels partners bij adviesbureau Het Management Centrum. Het betreft het zogenaamde Haalbaarheidsonderzoek *Centraal Ingericht Dynamisch Reisdocumenten Informatie- en Verificatie Systeem* (okt. 2003), ookwel *DRIVeS*. Opdrachtgever van deze haalbaarheidsstudie is BPR. De opdracht betreft "*het uitvoeren van een haalbaarheidsonderzoek naar een centraal ingericht Dynamisch Reisdocumenten Informatie- en Verificatie Systeem (DRIVeS) ter vervanging van het huidige Basisregister Reisdocumenten*", wat later de ORRA zou worden.

De achtergrond waartegen dit onderzoek zich afspeelt wordt alsvolgt toegelicht.

> *"Het agentschap BPR van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties overweegt om het huidige negatieve register (in de zin dat alleen documenten staan geregistreerd die niet in omloop mogen zijn) om te vormen tot een positief register.*
> *De belangrijkste reden die aan deze overweging ten grondslag ligt is de toenemende druk -nationaal en internationaal - om te kunnen voorzien in adequate informatie ter ondersteuning van het uitgifte- en controleproces en de opsporing met het oog op het terugdringen van identiteitsfraude."*[53]

Het algemene doel van DRIVeS is het volgende.

> *"Het ondersteunen van het werkproces bij de uitgifte van reisdocumenten en het verbeteren van de verificatie van Nederlandse reisdocumenten door opsporingsinstanties en door publieke en private organisaties die op grond van een wettelijke taak identiteitsverificaties verrichten."*[54]

Met betrekking tot de biometrie lijkt *DRIVeS* in een bredere doelstelling te voorzien. Dit lijkt een van de eerste documenten te zijn waarin de centrale opslag van biometrie als voorwaarde wordt gesteld en waarin opsporing als mogelijke functie wordt genoemd.

53 *DRIVeS*, versie1.0 definitief, 20 oktober 2004.
54 Idem.

*"Voor het effectief gebruik van biometrie in het uitgifteproces van documenten is de opslag in een centrale database voorwaardelijk. De ontwikkeling van DRIVeS kan de biometrische toetsing bij het uitgifteproces van documenten goed faciliteren. Alhoewel de doelstelling van DRIVeS daarin niet primair voorziet, is het denkbaar dat onder strikte juridische voorwaarden de biometrie die is opgeslagen in DRIVeS ook kan worden gebruikt t.b.v. terrorismebestrijding en opsporing."*[55]

Deze passage toont aan hoe dicht de verschillende doelstellingen technisch gezien tegen elkaar liggen, op het moment dat een systeem als *DRIVeS* eenmaal biometrische gegevens bezit.

In de volgende passage wordt gewezen op het fundamentele karakter van de omslag die ontstaat wanneer *DRIVeS* als politieinformatiesysteem gebruikt zou gaan worden.

*"Het huidige Basisregister Reisdocumenten is een register waar de Wet bescherming persoonsgegevens (Wbp) op van toepassing is. Indien de bevraging, nationaal en internationaal, zich verder ontwikkelen in de richting van steeds uitgebreidere bevraging in de vorm van rechercheren, dan zou DRIVeS de kant op kunnen gaan van een politie-informatiesysteem, waar de Wet op de politieregisters op van toepassing dient te zijn. Dat zou dus een fundamentele omslag zijn."*[56]

Hoewel eerst wordt gesteld dat *DRIVeS* een 1:n zoekfunctie op basis van uitsluitend de biometrie niet primair ondersteunt (behalve ten behoeve van off line de-duplicatie), wordt even verderop gezegd dat dit technisch wel mogelijk is.

*"Is in het kader van uitzonderlijke situaties toegang tot de opgeslagen biometrische informatie noodzakelijk, dan kan er op een biometrisch kenmerk gezocht worden in het register zonder dat dit gekoppeld is aan een document of aan een persoon."*[57]

De overwegingen voor centrale opslag zijn des te opvallender, omdat deze optie in de periode 1999 tot circa 2004 zeer resoluut van de hand werd gewezen om redenen van privaycbescherming. In het rapport *Onderzoek naar de toepassing van biometrische*

55 Idem.
56 Idem.
57 Idem.

*kenmerken voor Nederlandse reisdocumenten* van 16 juni 2003[58] (zie paragraaf 8.7) wordt het volgende gesteld.

> *"Voor vergelijking van het afgenomen biometrische kenmerk met in een database opgeslagen kenmerken is om redenen van privacybescherming niet gekozen."*

Ten tijde van het voorstel tot de wetswijziging in 2002[59] werd centrale opslag niet overwogen, in elk geval niet in de publieke discussie. Sterker, het wetsvoorstel sluit het uit door alleen over verificatie te spreken. Het toen pas opgerichte Agentschap BPR (onderdeel van BZK) wilde volgens Lies de Leeuw, voormalig medewerker van BPR, van een centrale oplossing niets weten.

> *"Het woord database was taboe. Er mocht niet over gepraat worden. Ik heb dat gevraagd omdat de fraude zich verplaatst. We zetten straks iets op de chip. Over vijf jaar komt iemand anders om een paspoort aan te vragen of af te halen en rommelt met de biometrie. Hoe gaan we dat voorkomen? Hoe gaan we de integriteit van de vingerafdruk borgen, gezien hetgeen de overheid ermee wil bereiken? Kunnen we dit borgen zonder centrale opslag? Dit zijn een paar vragen waar toen iedereen overheen is gevallen. Niet vanuit het idee "waar gaat dat heen met de privacy", want bij niemand was er het gevoel dat hij dáár wakker van lag. Het was meer de vraag "doen wij de politiek correcte dingen."*[60]

Een argument van internationaal karakter voor het aanleggen van een centraal reisdocumentenregister, zoals aangevoerd onder het kopje 'Internationale Ontwikkelingen' op pagina 12 van *DRIVeS*, zou het plan van de Europese Commissie zijn om een Europees paspoortenregister aan te leggen. Deze plannen zijn echter in een vroeg stadium gesneuveld onder andere vanwege grote bezwaren van lidstaten en het Europese Parlement. Daarbij vormde de bescherming van de privacy een belangrijk argument.

Waar eerdere studies geen uitspraken hebben gedaan over criteria voor de prestaties en betrouwbaarheid van het beoogde biometriesysteem, zou men dat bij deze

58 BPR (2003).
59 Wijziging van de Paspoortwet, onder andere in verband met het toepassen van biometrie in reisdocumenten 28 342 (R 1719), Tweede Kamer der Staten-Generaal KST61524, 2002, http://www.identificatieplicht.nl/doc28342.html.
60 WRR-interview 1 april 2010.

haalbaarheidsstudie juist wel verwachten. Het is dan ook onduidelijk op basis van welke onderzoeken en feiten in de conclusies op pagina 48 wordt gesteld dat *"met de beschikbare techniek de realisatie van DRIVeS haalbaar is zoals voorgesteld"*. Het rapport beperkt zich tot de uitspraak dat in technisch opzicht de toevoeging van biometrie in het centrale systeem slechts meer opslagruimte nodig heeft. Een tamelijk triviale constatering, wanneer men dat vergelijkt met de enorme uitdagingen die er liggen om de gehele bevolking biometrisch te registreren.

Verdere observaties met betrekking tot DRIVeS zijn:.

- De politiek/maatschappelijke acceptatie wordt volgens DRIVeS als geen enkel probleem gezien. Het het blijft onvoldoende duidelijk waar die uitspraak op is gebaseerd. Alle tot dan toe bekende studies en proeven waren immers uitgegaan van uitsluitend verificatie aan de hand van de biometrie op het paspoort.
- De (mogelijke) gevolgen van *DRIVeS* voor de privacy van de Nederlandse burgers worden niet besproken. Blijkbaar is het geen onderdeel geweest van het totaal aan afwegingen.
- De rapportage richt zich vrijwel uitsluitend op procedurele en functionele aspecten. Dit hebben we eerder gezien bij voorgaande studies en pilots. Met betrekking tot de biometrie worden geen criteria genoemd voor de prestaties en veiligheid. Haalbaarheid op die punten wordt dan ook niet aangetoond.
- De vraag of de kwaliteitseisen voor een identificatiesysteem (1:n) niet anders zijn dan voor het tot dan toe altijd beoogde verificatiesysteem (1:1) wordt niet gesteld. Het werd blijkbaar niet als een mogelijk probleem gezien. In het algemeen komt het rapport eerder over als een gedetailleerd projectplan dan een haalbaarheidsstudie.

### *8.9 Evaluatierapport Biometrieproef '2b or not 2b' (2005)*

Op 19 maart 2003 kondig minister Thom de Graaf van Bestuurlijke Vernieuwing en Koninkrijksrelaties een biometrieproef aan. Er was over de werking van biometrische apparatuur weliswaar veel (buitenlands) onderzoeksmateriaal aanwezig, maar dat had niet direct betrekking op de toepassing die de Nederlandse overheid voor ogen had. Daarom stond nog niet vast welke nieuwe handelingen de medewerkers van de uitgevende instanties moesten gaan verrichten, hoeveel extra tijd deze handelingen

gingen vergen en welke invloed dit had op de bestaande capaciteit van deze instanties. In zijn aankondiging zegt hij verder:

> *"Tevens zijn er onvoldoende gegevens over de robuustheid en betrouwbaarheid van biometrische apparaten in de aanvraag- en uitgifteprocessen van reisdocumenten, alsmede over de beheerslast die daarmee gemoeid zal zijn."*[61]

Dit laatste refereert aan veiligheidsaspecten van de techniek en de processen. Dit is relevant, omdat we per slot van rekening het aanvraag- en uitgifteproces veiliger willen maken en identiteitsfraude willen bestrijden. De proef vindt uiteindelijk plaats van 30 agustus 2004 tot 28 februari 2005. Zes gemeenten hebben aan de proef meegewerkt. Op vrijwillige basis hebben burgers parallel aan een reguliere paspoortaanvraag een proefpaspoort aangevraagd, waarop een gelaatsscan en (toen nog) 2 vingerafdrukken in een chip werden opgeslagen.

Nadat de proef heeft plaatsgevonden, kondigt toenmalig minister van BV&K Pechtold op 18 april 2005 het evaluatierapport van de proef aan. Hij doet dat alsvolgt.

> *"De proef is goed verlopen. De zes gemeenten hebben met veel inzet en enthousiasme meegewerkt aan de proef. In totaal zijn 14 779 biometrische testdocumenten geproduceerd voor de proef. Gepland waren ca. 15 000 documenten. De proef wordt thans geëvalueerd. In die evaluatie staan de volgende vragen centraal:*
>
> - *Welke praktische gevolgen heeft invoering van biometrie op de reisdocumenten voor de uitgevende instanties van de reisdocumenten;*
> - *Doen zich problemen/knelpunten voor (bijvoorbeeld ten aanzien van de bouwkundige voorzieningen, de beoordeling van de kwaliteit van de opgenomen biometrische kenmerken, etc.).*
>
> *De afronding van de evaluatie is begin mei 2005 gepland."*[62]

De bovengoemde brief werd overigens vergezeld van een aantal bijlagen, waaronder een beknopte rapportage van de kleinschalige pilots uit de periode 2000-2001 (zie paragraaf

61 Brief minister BV&K aan de Tweede Kamer, 19 maart 2003, kenmerk BPR2003/U87221
62 Brief minister BZ&K 18 april 2005, *Kamerstukken II*, 2004–2005, 25764, nr. 26.

8.4) en het eveneens eerder in dit deel besproken *Onderzoek naar de toepassing van biometrische kenmerken in de Nederlandse reisdocumenten* van 6 juni 2003.

Wat in de brief van Pechtold direct opvalt is dat de vraagstelling van 19 maart 2003 over de robuustheid en betrouwbaarheid van de biometrische apparatuur niet meer wordt genoemd. Verder worden we natuurlijk nieuwsgierig wat er met 'goed' wordt bedoeld, met name welk criterium daarvoor heeft gegolden en of het 'goed genoeg' is.

Later in 2005 verschijnt het evaluatierapport.

Allereerst zien we wederom een andere omschrijving van het doel van de proef.

> *1. na te gaan hoe het aanvraag- en uitgifteproces ingericht moet worden wanneer er biometrische kenmerken worden opgenomen;*
> *2. te toetsen of de biometrische kenmerken (gelaatscan en vingerscan) in de reisdocumenten geverifieerd konden worden.*[63]

Het zijn subtiele verschillen, maar het lijkt erop alsof de doelstellingen steeds beperkter worden. In elk geval is er geen aandacht besteed aan de fraudebestendigheid van de biometrische apparatuur en daarmee samenhangende processen. Met betrekking tot het tweede doel, namelijk of de biometrische kenmerken kunnen worden geverifiëerd, worden er volstrekt geen eisen gesteld. Het is te vergelijken met een onderzoek naar de vraag of een bepaald nieuw model auto ook achteruit kan rijden. Voor een systeem dat de identiteitsfraude moet terugdringen en dat een middel moet zijn in de strijd tegen terrorisme is dat van een verbazingwekkende oppervlakkigheid.

Verder is er gekozen om het geheel maximaal binnen het bestaande proces te laten verlopen. Dat hoeft op zichzelf geen probleem te zijn, ware het niet dat er geen vooraf gestelde doelen zijn gesteld ten aanzien van prestaties, kwaliteit, integriteit en veiligheid. Al deze criteria worden met die keuze dan ondergeschikt aan het bestaande proces.

63 BZK (2005).

Vervolgens komt er een verrassing: onderaan p. 11 staat dat er ook een interoperabiliteitstest wordt gedaan. Hier is in de Kamerstukken niet eerder over gesproken.

> *"Bij de proefgemeenten zijn ook de biometrische kenmerken geverifieerd met gebruikmaking van andere apparatuur dan de apparatuur die is gebruikt voor het opnemen van de biometrische kenmerken. Gebruik is gemaakt van apparatuur en programmatuur van zes leveranciers van biometrische verificatiesystemen (vingerscanner: Precise Biometrics, Nec, BioScrypt en Identix en camera: Biodentity, Cognitec en Identix).*[64]

Vanwege het gebrek aan (bruikbare) standaards en interoperabiliteit is dat een bijzonder grote uitdaging. Om dergelijke tests betrouwbaar uit te voeren is diepgaande kennis nodig van de techniek en van het testen van technology. De leveranciers hebben namelijk niet alleen verschillende opvattingen over kwaliteit, maar ook over de plaatsing van de kenmerken (zie ook Deel I en II). Bovendien is de software van de leveranciers als het ware gecalibreerd op hun eigen hardware en testdatabases. Dat geldt ook voor de matchingsoftware en de kwaliteitsoftware. De kwaliteitsoftware van het NIST die tijdens de proef is gebruikt voor de registratie, hoeft niet door de andere leveranciers te zijn gebruikt. En als dat wel zo is, dan is ook deze NIST-tool getraind op testdata van de leverancier. In dat verband zijn de volgende passages interessant.

> *"Voorafgaande aan de proef hebben de leveranciers, op grond van eigen testen, de grens ingesteld wanneer een vergelijking tussen kenmerken als succesvol of mislukt moest worden beoordeeld."*[65]

> *"De invoering van de kwaliteitsparameter bij de opname van de vingerafdrukken heeft geen eenduidig effect gehad op de verificaties door de andere verificatiesystemen dan bij het verificatiesysteem waarmee ook de opname van de vingerafdrukken is uitgevoerd. Dit effect wordt mogelijk*

64 Idem.
65 Idem, p. 44.

*veroorzaakt doordat opname- en verificatieprogrammatuur van één leverancier in samenhang wordt ontwikkeld."*[66]

Wanneer elke leverancier alleen voor de verificatie met zijn eigen drempelwaarden heeft gewerkt, zijn de reslutaten nauwelijks zinvol met elkaar te vergelijken. Er wordt dan letterlijk met twee maten gemeten. Zeker bij plaatjes van minder goede kwaliteit gaat de interpretatie van de kenmerken tussen leveranciers uit elkaar lopen. Zo kunnen de prestaties behoorlijk uit elkaar gaan lopen wanneer componenten van verschillende leveranciers worden gecombineerd. Een ander punt is dat de keuze voor een bepaalde drempelwaarde voor de kwaliteit er niet zomaar een is die de leverancier zelf kan kiezen. Het is een strategische keuze die afhangt van het complex aan afwegingen rond de afhandeling van de processen en gewenste mate van betrouwbaarheid. Door de leverancier de drempelwaarden te laten bepalen, heb je een van de belangrijkste sturingsmechanismen van de gehele toepassing uit handen gegeven. Bovendien zal een leverancier eerder proberen om de FRR laag te houden, omdat dan het proces minder wordt verstoord.

Het rapport is niet geheel duidelijk over de gebruikte registratieapparatuur. Waarschijnlijk zijn alle vingerafdrukken geregistreerd met apparatuur van Sagem (nu Morpho). Dat betekent dat Sagem als een soort referentie heeft gefungeerd. De prestaties van de andere leveranciers zeggen dan meer over de mate van interoperabiliteit met – in dit geval – Sagem dan over de prestaties op zich. Hier manifesteert zich het fenomeen van leveranciersafhankelijkheid, al wordt die conclusie in de rapportage niet zo vermeld.

Het testen van interoperabiliteit tussen vingerafdruckleveranciers is een bijzonder lastig en arbeidsintensief project. Daarvoor zijn diepgaande kennis over de technologie en over gespecialiseerde testmethoden een absolute voorwaarde, alsmede volstrekte onafhankelijkheid. Er zijn bovendien onafhankelijk gevalideerde testdatabases voor nodig, plus door alle partijen geaccepteerde referenties voor image quality en de plaatsing van de kenmerken (minutiae). In dit geheel speelt vervolgens ook nog de gewenste betrouwbaarheid een rol. Is die hoog, dan mogen uiteraard de marges tussen de verschillende opvattingen over kwaliteit en de plaatsing van kenmerken niet te veel

66 Idem, p. 45.

verschillen. Projecten als MINEX (www.nist.gov/itl/iad/ig/minex.cfm ) en MTIT (www.mtitproject.com) zijn daar per test al snel twee jaar mee bezig.

Een ander punt met de proef '2b or not 2b' is dat de FAR niet is onderzocht. Er is niet gekeken naar mogelijkheden tot fraude of frustratie van het systeem door kwaadwilligen. Die risico's zijn niet in kaart gebracht, noch weten we wat we eraan moeten doen om die te verkleinen. Dientengevolge kunnen we geen schatting doen van de mate waarin de biometrie een bijdrage zal kunnen leveren aan het terugdringen van identiteitsfraude en 'look alike fraude' in het bijzonder. Ruud van Munster zegt hierover:

> *"Ook tijdens 2b or not 2b heb ik me verbaasd over de relatief geringe aandacht voor de prestaties. De nadruk lag erg op het proces."*[67]

In het kader van deze WRR-studie heeft er op 18 februari 2010 een interview plaatsgevonden met Arnout Ruifrok, wetenschappelijk onderzoeker beeldonderzoek en biometrie bij het Nederlands Forensisch Instituut (NFI). Het NFI werd destijds bij '2b or not 2b' enkele keren zijdelings betrokken, waaronder eenmaal op het moment dat het testprogramma al was vastgelegd en later nog eens, toen de proef achter de rug was en de testresultaten moesten worden geïnterpreteerd. Het blijkt dat hij destijds de nodige gebreken in de opzet en uitvoering van de proef constateerde.

> *"Als je van uitgebreide testen iets wil leren, moet je vooral ook opschrijven wat er fout gaat. Men is geneigd te rapporteren wat er goed gaat. Soms worden vingerafdrukken meerdere malen aangeboden voordat het goed gaat. Dan wil ik weten: waarom is het de keren daarvoor fout gegaan, en hoe vaak is dat geweest?" Juist van de dingen die misgaan leer je immers. De rapportage van '2b or not 2b' komt er eigenlijk op neer dat "als we een heleboel slechte vingerafdrukken niet meerekenen, dan werkt het systeem best wel goed!"*[68]

In het interview noemt Ruifrok als grote gemiste kans van de proef het feit dat niet is gewerkt met de grote aantallen vergelijkende data en curven die normaal gesproken uit performance tests met grote systemen of databases voortvloeien. Dergelijke data en curven van '2b or not 2b' bestonden volgens Ruifrok wel, maar zijn niet opgenomen in de

67 WRR-interview, Den Haag, 16 februari 2010.
68 WRR-interview, 18 februari 2010.

eindrapportage. Probleem was verder dat alle data die tijdens de proef gegenereerd waren, vervolgens niet inzichtelijk konden worden gemaakt. In een algemeen commentaar van het NFI op de concept-rapportage '2b or not 2b' van destijds is onder het kopje 'praktische bruikbaarheid' onder andere genoteerd dat:

> *"het onduidelijk is of het alleen gaat om de vraag of implementatie technisch mogelijk is of ook om de vraag of de performance een bepaald niveau haalt. Het rapport maakt de indruk zeer compleet te worden, maar daardoor komen soms ook belangrijke punten in de verdrukking. Er lijken meerdere auteurs bezig te zijn, en in een eindversie zal nog moeten worden bekeken in hoeverre dezelfde informatie meerdere malen in andere bewoordingen voorkomt."*[69]

Uit de gegenereerde data moest het NFI onder andere min of meer achteraf gokken welke drempelwaarden er tijdens de proef waren gehanteerd. Verder zaten er volgens Ruifrok rare verdelingen van meetwaarden tussen en was soms niet goed te zeggen "*wat ze nou eigenlijk gedaan hadden"*. Ook uit de resultaten van de scores met vingerafdrukvergelijkingen (tussen verschillende fabrikanten*) "kon geen chocola gemaakt worden"*. Op basis van die resultaten zijn vervolgens echter wel beslissingen genomen. Verder bleken er rare verschillen in resultaten te bestaan tussen dezelfde systemen bij verschillende gemeenten. Overigens werd het NFI pas bij een en ander betrokken nadat de proef al liep. Er is daarom geen sprake geweest van enige directe invloed van het NFI op de opzet en uitvoering van de proef.

Halverwege de proef zijn de drempelwaardes (thresholds) veranderd. Ruifrok zegt daarover:

> *"Van '2b or not 2b' had ik graag (offline) analyse van de data gezien; pas dan kan je goed (ROC) curves van combinaties van verschillende componenten bepalen. Dan is het ook niet nodig of storend als halverwege een experiment thresholds veranderd worden. Echter in dit project moesten we het doen met beperkte informatie (alleen de matchwaardes van de verificatie bij aanvraag en uitgifte, geen 'identificatie' ofwel matching tegen andere vingers/gezichten in de database). Analyse achteraf van onvolledige en deels onbetrouwbare resultaten is natuurlijk nooit een goede zaak. Nou was het experiment natuurlijk opgezet*

69 WRR-interview, 18 februari 2010.

*om 'functionele interoperabiliteit' te testen, en performance niet de focus van de test, [dus] leek de analyse een 'afterthought'."*[70]

Omdat tijdens de proef alleen maar verificaties zijn uitgevoerd ten opzichte van de opgeslagen data in de chip, zegt de proef nagenoeg niets over de te verwachten prestaties bij een toekomstige 1:n zoekactie (zie Deel I, paragraaf 1.8 'Invloed van kwaliteit op de nauwkeurigheid van de matcher'). Na de praktijkproef '2b or not 2b' zijn er geen haalbaarheidsstudies of proeven meer geweest, ondanks dat in het politieke debat sinds 2005 de functie van de biometrie significant is uitgebreid. Er lijkt een blind geloof te bestaan in de techniek, want de vraag of de biometrische techniek in de context van de nieuwe Paspoortwet wel kan gaan functioneren is nooit beantwoord.

Tot slot nog een enkele opmerking over de geteste gezichtsherkenningsapparatuur. Over de prestaties van de twee verschillende methoden, te weten scannen van de foto en de livescan, concludeert het rapport het volgende.

*"De gelaatscan die tot stand komt door de foto te scannen heeft in de proef geleid tot circa 4% uitval bij verificatie. Deze uitval wordt onder andere veroorzaakt door de resolutie waarmee de foto is gescand (300 dpi). Een andere oorzaak voor de uitval is dat de foto, voor automatische gelaatsherkenning, moet voldoen aan strengere eisen dan die nu worden gesteld aan de foto. De uitval bij verificatie van de gelaatscan die op basis van een livescan is gemaakt bedraagt 0,1%."*[71]

Blijkbaar zijn er verkeerde eisen gesteld aan de foto's van het gelaat. Dat is natuurlijk jammer, want dat betekent dat de proef voor niets is uitgevoerd. Wel blijkt de livescan maar liefst 40 maal beter te presteren dan de gescande foto. Als men trouw zou zijn aan de uitgangspunten, namelijk het betrouwbaarder maken van het aanvraag- en uitgifteproces, dan zouden we onmiddelijk de livescan moeten invoeren. Dat is niet gebeurd omdat de fotobranche teveel omzet zou gaan mislopen. Of omdat het invoeren van de livescan te grote investeringen zou vragen?

70 WRR –interview, 18 februari 2010.
71 Evaluatierapport Biometrieproef '2b or not 2b', BZK (2005).

Tot slot is het woordgebruik niet helder. 'Uitval bij verificatie' is geen gangbare term in de biometrie. Aannemelijk is dat hiermee de FRR wordt bedoeld, maar duidelijk is het niet.

## 9. De techniek in het debat

Het wetgevingsproces heeft in totaal circa negen jaar geduurd. Het actief overwegen van biometrie ter bestrijding van 'look alike fraude' is begonnen met de studie van TNO in 1999 en vond zijn definiteve weerslag in de goedkeuring van het nieuwe wetsvoorstel door de Eerste Kamer op 9 juni 2009.

Uit het vorige hoofdstuk blijkt hoe dun de bewijzen zijn dat we met het biometrische paspoort technisch gezien op de goede weg zijn. Desondanks bleven in het politieke debat de verwachtingen zich opstapelen. Daar waar de ICAO met Doc9309 en later de Europese Unie met EC2252/2004 kozen voor opslag uitsluitend in het reisdocument, was dit voor Nederland onvoldoende. Zich niet goed realiserend dat binnen de relatief beperkte scope van EC2252/2004 een veelheid aan fundamentele uitdagingen zat (met name in het aanvraag- en uitgifteproces), is Nederland verder gaan bouwen en is er een nationale kop gecreëerd bovenop de Europese verordening. Er was de indruk ontstaan dat de Europese verordening niet voldoende veiligheid kon waarborgen en dat centrale opslag randvoorwaardelijk was. Nederland nam daarmee binnen Europa een koplopersfunctie. De verantwoording daarvoor gebeurde vanuit de overheid soms met krachtige taal. Zo doet toenmalige minster van BV&K Alexander Pechtold de volgende uitspraken over de noodzaak tot het centraliseren van de reisdocumentenadministratie en de vingerafdrukken.

> *"In het kader van de **bestrijding van terrorisme** is het van het grootste belang dat voorkomen wordt dat **terroristen** de identiteit kunnen aannemen van andere personen en als gevolg daarvan onopgemerkt blijven."*
> *.../...*
> *"Inzake de **bestrijding van terrorisme** is aangegeven dat de on line verificatie veronderstelt dat de administraties van de identiteits-documenten met biometrische kenmerken centraal zijn georganiseerd."*
> *.../...*

> *"Gelet op de maatregelen die het kabinet noodzakelijk acht in het kader van de* ***bestrijding van terrorisme en identiteitsfraude*** *ben ik van plan het zuiver decentrale karakter van de reisdocumentenadministratie te wijzigen en tot centralisatie van de administratie over te gaan."*[72]

De context waarbinnen de biometrie moet gaan functioneren, wordt steeds ambiteuzer en complexer. Daarmee worden de verwachtingen ten aanzien van de toegevoegdewaarde van biometrie binnen die context steeds veeleisender.

Nu we naar aanleiding van voorgaande delen van deze studie hebben gezien welke grote uitdagingen er op het vlak van de technische implementatie nog spelen en welke fundamentele onzekerheden er nog steeds bestaan over de veiligeheid, betrouwbaarheid en prestaties van de biometrische techniek en de processen die daarmee samenhangen, wordt zichtbaar dat er door de jaren heen een steeds groter wordende kloof is ontstaan tussen de techniek en de groeiende ambities rond het gebruik van die techniek.

In de parallelstudy *Happy Landings?* van Vincent Böhre wordt uitgebreid ingegaan op de diverse stadia van het politieke besluitvormingsproces. Böhre geeft een uitvoerig overzicht van de door de overheid uitgezette lijnen en de metamorfose die het biometrische paspoort sinds 1999 heeft ondergaan. Om toch op compacte wijze een beeld te schetsen van hoe de techniek door de overheid en politiek in het debat is behandeld volgen hieronder een paar korte illustraties.

### *9.1 Eerste Kamerdebat 9 juni 2009*

Tijdens het Eerste Kamerdebat op 9 juni 2009, de datum dat de wet in zijn huidige vorm werd goedgekeurd, zijn door senatoren diverse kritische vragen gesteld. Als een soort apotheose passeren op het laatste moment nog eens alle belangrijke bedenkingen en argumenten de revue.

72 Brief van de minister van BV&K, 18 april 2005, *Kamerstukken II* 25 764, nr. 26.

Allereerst nemen we de koplopersrol van Nederland in Europa, een belangrijke katalysator van de groeiende verwachtingen. Daarover zegt mevrouw Strik (GroenLinks) het volgende.

> *"../.. Omdat het gebruik en de opslag van biometrische gegevens in paspoorten allang een Nederlands paradepaardje was dat de regering per se in de Europese stal opgenomen wilde zien. De Europese lobby begon al onder D66-minister Van Boxtel en is sindsdien met verve gevoerd door onder andere de ministers De Vries en Pechtold. ../.. Overigens zou het mij niet verbazen als de regering zich misschien laat verleiden de euroscepsis nog een handje te helpen door dit wetsvoorstel te verkopen als iets dat "moet van Brussel", hoezeer wij ook aan de wieg hebben gestaan en hoeveel extra's wij nu ook aan de implementatiewet hangen."*[73]

En dat Nederland inderdaad die voortrekkersrol ambieerde blijkt uit het volgende citaat uit 2003.

> *"Een belangrijke rol in de ontwikkeling en vormgeving van de voorstellen aangaande biometrie in de paspoorten door de Europese Commissie kan naar verwachting vervuld worden door het European Forum for Travel Documents dat in 2002 op initiatief van Nederland is opgericht om op het gebied van reisdocumentenaangelegenheden samenwerking in Europees verband vorm te geven."*[75]

Jarenlang heeft Agentschap BPR het voorzitterschap dan wel het secretariaat van het forum gevoerd. Ook beheerde het agentschap in elk geval tot voor kort de website van het forum, dat inmiddels is omgezet in het International Forum for Travel Documents.

Over de veiligheid van de biometrische techniek zegt mevrouw Strik gedurende datzelfde debat op 9 juni 2009:

> *"Naast de beveiligingsrisico's is ook de foutmarge bij opslag een risicofactor. Vier jaar geleden ging het verifiëren van vingerafdrukken nog in 3% van de gevallen fout."*[76]

73 Stenogram Eerste Kamerdeabt, 9 juni 2009, http://www.eerstekamer.nl/stenogram/stenogram_261/f=/vi61mouk9cnh.pdf.

Zoals we hebben gezien in het vorige hoofdstuk is de veiligheid bij geen enkele proef of studie op grondige wijze onderzocht. Uitzonderingen hierop zijn de twee studies van TNO in respectievelijk 1999 (*Alle mensen zijn Ongelijk*) en 2002 (*Biometrics "Against Look Alike Fraude"*), die met name de risico's en leemtes in de technologie hebben vastgesteld. Wat de mislukte verificaties betreft: de genoemde 3% zou nog wel eens aan de optimistische kant kunnen zijn. Het NFI had namelijk nogal wat kritiek op de kwaliteit van de uitvoering en de verwerking van de testdata van de proef '2b or not 2b'. Bovendien was dit percentage alleen maar mogelijk indien consequent alle apparatuur van uitsluitend één leverancier gebruikt werd. Het uitwisselen van (delen van) de apparatuur van andere leveranciers bleek foutpercentages op te leveren die tussen 15% en 30% lagen, met hier en daar uitlopers naar boven de 50%.[74] Dit laat zien dat er op het punt van interoperabiliteit nogal wat uitdagingen lagen. Voor meer resultaten uit de praktijk wordt verwezen naar het rapport *UK Passport Service Biometrics Enrolment Trial* uit 2005, uitgevoerd door Atos Origin. Daar wordt voor vingerafdruk een FRR van rond de 20% gemeld.[75]

Na tien jaar van voorbereiding kan staatssecretaris Bijleveld van Binnenlandse Zaken en Koninkrijksrelaties het volgende zeggen over de veiligheid.

> *"Woordvoerders hebben gevraagd hoe groot de kans is dat een vingerafdruk bij een verkeerde persoon in het reisdocument terechtkomt in de administratie. Die kans acht ik niet groot. Alle procedures, en ook de technische voorzieningen zoals de biometrische zoekfunctie in het centrale bestand, zijn zo ingericht dat dit moet worden voorkomen[76]."*

Tenzij er niet-openbare proeven en studies zijn verricht buiten hetgeen er aan de Tweede Kamer is gerapporteerd, lijkt er weinig op te wijzen dat de technische voorzieningen en procedures op het punt van veiligheid, betrouwbaarheid en integriteit grondig zijn getest, laat staan ontworpen. En als het proces aan de balie niet volledig is aangepast aan de

74 BZK (2005), tabellen 8 en 9 op p. 49.

75 http://hornbeam.cs.ucl.ac.uk/hcs/teaching/GA10/lec3extra/UKPSBiometrics_Enrolment_Trial_Report.pdf.

76 Idem.

noodzakelijke eisen van veiligheid, betrouwbaarheid en integriteit, zal de centrale functie nooit goed kunnen preseteren. In dat licht is het ook moeilijk te begrijpen waar de staatssecretaris haar volgende uitspraak op baseert:

> *"De nieuwe opzet van de reisdocumentenadministratie leidt tot een betrouwbaardere aanvraag en uitgifte van reisdocumenten. Daardoor wordt het ondermeer beter mogelijk om fraude met en misbruik van reisdocumenten te bestrijden."*[77]

Wat betreft de rol van biometrie in dat geheel laten geen van de studies en proeven zien wat precies de risico's zijn en hoe deze worden tegengegaan door de juiste inzet van techniek, processen en procedures.

In haar betoog noemt de staatssecretaris de waarborg die moet voorkomen dat er een zoekactie plaats kan vinden op basis van uitsluitend de biometrie.

> *"De officier van justitie moet het geslacht van de betrokkene weten en een gezichtsopname en vingerafdrukken hebben. Alleen met deze drie gegevens van een betrokkene zal de officier van justitie in geval van een misdrijf waarvoor voorlopige hechtenis is toegelaten. Wat wel kan, is dat van iemand die al achter de tralies zit en die zijn naam niet geeft maar van wie wel een foto en vingerafdrukken aanwezig zijn, de identiteit kan worden vastgesteld."*[78]

Deze waarborg hebben we vaker gehoord en klinkt geruststellend. Maar technisch gezien zitten er een paar onduidelijkheden in die daar potentiëel afbreuk aan kunnen doen. Want de zoekfunctie op basis van de foto gaat in zo'n grote database niet werken. Studies hadden uitgewezen dat 1:1 verificatie op basis van het gelaat al niet goed genoeg presteert (zie pargraaf 8.6 Technical Survey). Bij een 1:n zoekactie in een database van 17.000.000 foto's van zeer matige kwaliteit zullen de fouten vele malen groter zijn. Het lezen van het geslacht is 50% kans. De uiteindelijke zoekactie zal dan toch gebaseerd moeten zijn op de vingerafdrukken. De verdachte hoeft dan niet fysiek aanwezig te zijn: je neemt een hele slechte foto van een willekeurig iemand, van wie je weet dat daar honderden of duizenden hits op kunnen komen. Die kun je verder negeren. Je gokt het geslacht,

77 Idem.
78 Idem.

waarmee je in elk geval ca. 8.500.000 hits hebt. Komt er geen hit uit, dan probeer je het nog eens op basis van het andere geslacht en dan heb je toch de gehele bevolking op basis van de vingerafdrukken doorzocht.

> *"Het gaat steeds om identiteitsvaststelling; daar is deze databank voor! Ze [i.e. de vingerafdrukken] worden gebruikt in strafrechtelijk onderzoek ter vaststelling van de identiteit."*[79]

Is dit niet precies zoals de vingerafdrukken in bijvoorbeeld Havank worden gebruikt? De intentie is ongetwijfeld goed, maar het woordgebruik leidt tot verwarring.

Over het bewaken van de beveiliging zegt de staatsecretaris het volgende.

> *"Beveiligingsspecialisten zullen wij continu risico's laten monitoren."*[80]

In de bespreking van de studies en proeven hebben we gezien dat beveiliging en veiligheid een ondergeschikte rol hebben gespeeld. Diverse specialisten hebben moeite gehad hun stem te laten horen. Het resultaat is dat er nog steeds geen goed zicht is op de risico's. Arnout Ruifrok zegt hierover:

> *"Een aantal aspecten in het implementatietraject van de ORRA is inmiddels zo vrij zijn gelaten, dat het eerder makkelijker zal worden om frauduleus een paspoort aan te vragen dan moeilijker. Dit omdat het de baliemedewerker moeilijker wordt gemaakt om een goede controle uit te oefenen: er is 1) keuzevrijheid m.b.t. de vingerafdrukken die worden opgeslagen, en 2) die keuze voor bepaalde (in totaal 4) vingers wordt niet door het systeem onthouden, maar dient de burger zich bij controle zelf te herinneren. Kwaadwillenden zouden dus bijvoorbeeld twee keer achter elkaar een paspoort kunnen aanvragen door bij de tweede keer een fysieke beperking aan de eerder gebruikte vingers te veinzen."*[81]

Ruifrok noemt in het bovengenoemde interwiew verder nog enkele implementatieproblemen, zoals personen van wie niet alle opgenomen vingerafdrukken later blijken te matchen en verkeerd opgeslagen vingerafdrukken door onoplettend

79 Idem.
80 Idem.
81 WRR-interview, 18 februari 2010.

baliepersoneel. Verder zou in een eerder stadium het opslaan van tien vingerafdrukken disproportioneel geacht zijn (zie citaat minister Korthals uit 2001 in paragraaf 2.2 van Deel I van deze studie), terwijl dit een eventuele 1:n search juist ten goede zou zijn gekomen. Ook zijn er geen goede fallback-procedures. Het baliepersoneel kan eventueel alles overrulen en iemand ondanks problemen een paspoort meegeven. Verder noemt hij het risico van siliconen vingerafdrukken; het baliepersoneel dient daar erg alert op te zijn.

### *9.2 Evaluatie na 6 maanden*

In haar brief van 17 september 2009 aan de Kamer heeft staatssecretaris Bijleveld beloofd dat het ministerie van BZK nauwgezet het aangepaste aanvraag- en uitgifteproces zou volgen om zo inzicht te krijgen in de eventuele knelpunten die zich in de praktijk zouden kunnen voordoen.[82] Op 17 maart 2010 wordt die evaluatie per brief aan de Kamer gezonden.[83]

De evaluatie begint met het bespreken van de opleiding van medewerkers van de uitvoerende instanties. De opleiding wordt zowel klassikaal als digitaal aangeboden. Bemerkenswaardig is dat er een mate van vrijblijvendheid klinkt. Zo is de 'mogelijkheid' gegeven om de opleiding te volgen en is de opleiding ook digitaal gegeven. Dat laatste houdt in dat aan alle uitgevende instanties een cd-rom (*De Digitale Docent*) is opgestuurd. Ook is deze cd-rom kosteloos beschikbaar gesteld aan uitzendbureaus. In de evaluatie staat daarover:

> *"Een aantal uitzendbedrijven heeft aangegeven van het opleidingsmateriaal gebruik te zullen maken."*[84]

Deze vrijblijvendheid staat in schril contrast met het belang dat op beleidsmatig en politiek niveau voortdurend wordt gehecht aan het veiliger maken van het aanvraag- en uitgifteproces. Bovendien is zes jaar eerder tijdens de praktijkproef '2b or not 2b' al het volgende geconstateerd.

82 Kamerstukken II 2009-2010, 31 324 nr. 23.
83 Vingerafdrukken in Nederlandse Reisdocumenten, 17 maart 2010. Kenmerk BPR 2010/51674.
84 Idem

*"De gemeenteambtenaren die de training bij de producent hebben gevolgd blijken niet altijd de opgedane kennis aan hun collega's te hebben doorgegeven, onder andere vanwege tijdsdruk. Als gevolg daarvan is het voorgekomen dat ambtenaren onvoorbereid aanvragen en uitgiften van biometrische testdocumenten hebben afgehandeld. Verder is gebleken dat het schriftelijk verstrekte opleidingsmateriaal (zowel het opleidingsmateriaal dat voorafgaande aan de proef is uitgereikt als het aanvullende opleidingsmateriaal dat is verstrekt om het opnemen van de vingerafdrukken te verbeteren) op een enkele uitzondering na, gedurende de proef niet als naslagwerk is gebruikt."*[85]

Dat goed opgeleid baliepersoneel van groot belang is voor de kwaliteit en integriteit van het aanvraag- en uitgifteproces wordt op diverse plaatsen en door verschillende bronnen in deze studie bevestigd. Het mag langzamerhand zelfs de status van 'algemeen bekend' krijgen. Het is daarom jammer te moeten constateren dat ondanks de bevindingen uit 2005, er sindsdien geen strengenter beleid is ontwikkeld ten aanzien van de training van het baliepersoneel, zeker wanneer dat uitzendkrachten betreft. Met het oog op de evaluatie van de staatssecretaris moeten we constateren dat er op dat zeer belangrijke punt weinig structureels is ondernomen. Met de ambities van de overheid in beschouwing zou eerder certificering van personeel en opleiding in de lijn der verwachtingen liggen.

*De belangrijkste* graadmeter voor het bepalen van het succes van het biometrische afnameproces is de kwaliteit van de geregistreerde vingerafdrukken. Zoals we eerder hebben gelezen heeft Duitsland uitsluitend voor dat doel een centraal register opgezet waar uitsluitend de kwaliteitsparameters van de afgenomen vingerafdrukken worden opgeslagen. Dit is bijzonder nuttig bij het evalueren van de kwaliteit en de mogelijke oorzaken in gevallen dat de kwaliteit slecht is. De staatssceretaris zegt hierover:

*"../.. Het is immers van belang dat de vingerafdrukken goed worden opgenomen. Dat blijkt voor een deel van de ambtenaren best lastig te zijn. Opletpunten zijn met name dat de vingers goed op het apparaat worden gelegd om te voorkomen dat*

85 Evaluatierapport Biometrieproef '2b or not 2b', BZK (2005), p. 24.

*maar een deel van de vingerafdruk wordt opgenomen. Overigens merk ik hierbij op dat bij het overgrote deel van de aanvragen het opnameproces goed verloopt."*[86]

De evaluatie doet geen concrete uitspraken over de kwaliteit van de afdrukken, het type en oorzaak van fouten, incidenten van (poging tot) fraude, bezwaren en protesten. Er kan op basis van deze evaluatie nauwelijks worden bepaald of de doelstellingen worden bereikt en zo niet, wat er precies moet gebeuren om dat wel te kunnen.

Wel meldt zij een probleem met het afnemen van vingerafdrukken van ouderen. Daarbij wordt niet aangegeven hoe groot dat probleem precies is en wat de gevolgen van dat probleem (kunnen) zijn. Wel komt zij met een maatregel.

*"Gelet hierop heb ik laten nagaan of er in het aanvraagproces aanpassingen kunnen worden aangebracht om het opnemen van vingerafdrukken bij deze groep te vergemakkelijken. Ik zie inderdaad mogelijkheden daartoe door bij personen vanaf 70 jaar maar één opname per vinger te maken en niet (zie ook mijn brief van 17 september 2009) minimaal twee en maximaal drie opnames. Voor personen van 70 jaar en ouder wordt zo spoedig mogelijk het opnameproces in deze zin aangepast."*[87]

Uit het artikel van Uwe Siedel ('Germany puts Quality First', zie ook paragraaf 6.2) blijkt dat na meerdere pogingen de kwaliteit van de afgenomen vingerafdrukken verbetert ten opzichte van de eerste poging. Vanuit het oogpunt van kwaliteit zou aan deze groep van boven de 70 jaar juist meer tijd en aandacht besteed moeten worden. Daarbij is het de vraag welke minimale kwaliteit acceptabel is.

Overigens worden in de digitale cursus voor baliemedewerkers Digitale Praktijkopleiding Reisdocumenten "De digitale docent" (versie 2.1) geen instructies gegeven voor het herkennen van valse vingerafdrukken of andere vormen van manipulatie. Verder is de instructie met betrekking tot het verifiëren van de vingerafdrukken bij uitgifte van het paspoort geblokkeerd en is er de volgende mededeling voor in de plaats gekomen:

86 Vingerafdrukken in Nederlandse Reisdocumenten, 17 maart 2010. Kenmerk BPR2010/51674.
87 Idem.

*Het uitlezen van de chip en het verifiëren van de vingerafdrukken vindt alléén plaats als de ambtenaar van de uitgevende instantie twijfelt of de persoon die het document komt ophalen ook de aanvrager is.*[88]

Los van het recht dat de burger heeft om de opgeslagen data in te zien en deze eventueel te laten wijzigen indien ze incorrect blijken, zorgt het weglaten van de verificatie van de vingerafdrukken bij ontvangst dat 1) de prestaties niet kunnen worden gemeten en 2) de biometrie geen bijdrage levert aan het veiliger en betrouwbaarder maken van het uitgifte proces, een kerndoelstelling van het biometrische paspoort. De overheid heeft tot op heden nog geen afdoende uitleg gegeven voor het schrappen van die procedure.

### *9.3 Vragen Gemeenteraad Utrecht aan burgermeester*

Uit de hierboven besproken evaluatie is gebleken dat op diverse belangrijke vragen geen antwoord is gegeven. Dat de overheid karig is met antwoorden betekent niet dat de burgers geen behoefte aan duidelijkheid zouden hebben. Eerder het tegendeel: de burgers gaan zich steeds meer afvragen, omdat er een gevoel van onbehagen kan gaan ontstaan over hoe de zaken er nu precies voorstaan. Er kunnen twijfels gaan ontstaan over de intenties van de overheid, maar ook simpelweg of de overheid haar zaakjes wel goed regelt. Het gaat per slot van rekening over een gevoelige kwestie als het afnemen en opslaan van vingerafdrukken van burgers.

Op 19 november 2010 heeft Klaas Verschuure, lid van de gemeentraad van Utrecht van D66, een reeks vragen ingediend met betrekking tot het afnemen, opslaan, gebruik en beveiliging van de biometrische gegevens. Hier volgt een selectie.

- *Welke voorzorgsmaatregelen zijn genomen om te voorkomen dat iemand "valse" vingerafdrukken gebruikt?*
- *Hoe wordt gecontroleerd of de afgenomen vingerafdrukken correct zijn?*
- *Hoe wordt gecontroleerd of de afgenomen vingerafdrukken correct in het paspoort zijn opgenomen?*

[88] Digitale Praktijkopleiding Reisdocumenten "De digitale docent" (versie 2.1)

- *Gebeurt deze controle bij elk individueel persoon, zo ja hoe en zo nee waarom niet?*
- *Hoe wordt gecontroleerd of de afgenomen vingerafdrukken correct worden opgenomen in de database?*
- *Welke functionarissen zijn bevoegd tot het afnemen van de vingerafdrukken en hoeveel personen zijn dat?*
- *Welke eisen worden aan deze functionarissen gesteld en hebben zij daartoe een opleiding moeten volgen?*
- *Welke beveiligingsmaatregelen zijn getroffen om onbevoegde toegang tot de database te voorkomen?*
- *Wanneer iemand geen of geen goede vingerafdrukken kan afgeven, hoe wordt dat dan opgelost?*
- *Deelt u de mening van D66 dat de opslag van vingerafdrukken in een database geen toegevoegde waarde heeft wanneer deze niet allemaal gecontroleerd worden. Immers bij vervuiling en fouten kan niet meer met zekerheid van de gegevens uitgegaan worden.*

Het interessante van deze vragen is dat veel van de onderliggende problematiek al in 1999 in het rapport van TNO werd onderkend. Blijkbaar is er in tien jaar van ontwikkeling aan de hand van studies, pilots en proeven onvoldoende antwoord gegeven op deze vragen en moeten deze nu via de lokale overheid alsnog aan de orde worden gesteld.

## 10. Conclusies Deel III

Tussen 1999 en 2004 zijn diverse studies en proeven gedaan. In de periode daarna is onder invloed van internationale en Europese ontwikkelingen in de naschok van 11/9 het politieke debat rond het biometrische paspoort in een stroomversnelling geraakt. 'Look alike fraude' is in een steeds breder perspectief komen te staan, terwijl de mogelijkheid om personen uitsluitend op basis van hun biometrische gegevens te kunnen identificeren tot de verbeelding sprak in justitiële en politionele kringen. Er ontstond een visie dat voor het breder aanpakken van identiteitsfraude en terrorisme de gegevens van de burgers centraal opgeslagen zouden moeten worden, inclusief de vingerafdrukken.

Echter, biometrie op nationale schaal is nieuw en het verkrijgen van een helder beeld van de mogelijkheden en risico's van het gebruik van biometrie voor kritische systemen als het paspoort was (en is) een lastige zaak. De eerste studies (onder andere van TNO) tussen 1999 en 2002 wijzen uit dat er vrijwel geen bruikbare gegevens bestaan over hoe de biometrische techniek zich gedraagt bij toepassing op dergelijke schaal. En de gegevens die er waren, betroffen laboratoriumtests die niet representatief waren voor een operationele toepassing. Daar kwam bij dat ook het soort toepassing nieuw was, waardoor de invloed van operationele factoren op de prestaties van een biometrisch systeem grotendeels onbekend was. De standaardisatie was nog maar net goed begonnen, dus onafhankelijk testen en certificeren van biometrische producten en systemen was zeker nog geen routine.

De eerste studies van TNO lijken een serieuze poging te zijn in het doorgronden van het kernprobleem. Er wordt gesproken over vormen van fraude en misbruik, en van het bepalen van cruciale zaken als de True Accept Rate en de True Reject Rate. Er wordt de vraag gesteld aan welke criteria het biometrische systeem eigenlijk moet voldoen en hoe het geheel moet worden ingericht om daaraan te kunnen voldoen. Bij zoveel onbekende factoren en variabelen is het een grote uitdaging om daar een sluitend antwoord op te vinden. Echter, zeker in de gegeven omstandigheden is het nalaten van die zoektocht een factor die het risico op verkeerde beslissingen verhoogt.

Het beeld dat zich vormt bij het overzien van de uitgevoerde studies en tests door de tijd heen is dat na 2003 men zich steeds meer ging richten op de processen en operationele aspecten. Vragen over veiligheid, fraude, fall back procedures, scenario's bij mislukte verificaties etc. worden nauwelijks meer gesteld. In de praktijkproef '2b or not 2b' komen deze zaken dan ook niet aan de orde. Met als gevolg dat we nu eigenlijk nog steeds niet weten hoe het systeem zal presteren. Veel meer richten de studies en rapportages zich op procesmatige en praktische zaken. Die begrijpen we beter en dus kunnen we daar makkelijker voor kiezen. Het gevolg is dat de veiligheid van het biometrische systeem en de daarmee samenhangende processen en procedures onderbelicht zijn gebleven. Weinig is er gepoogd een verband te leggen tussen de aard en omvang van het kernprobleem en de wijze waarop en de mate waarin men verwacht dat de biometrie kan bijdragen aan de

oplossing daarvan. Juist wanneer de technologie onbekend is moeten scherp geformuleerde eisen in elk geval leiden tot tests en proeven met een uitkomst die geëvalueerd kan worden. Op die manier leren we de techniek kennen en toepassen.

Een succesvol biometrisch systeem kent een strakke balans tussen technische en operationele parameters. Omdat deze elkaar sterk kunnen beïnvloeden, kunnen ze bij het bepalen van de eisen niet los van elkaar worden vastgesteld. De interactie tussen mens en sensor en het statistische karakter van de biometrische vergelijkingen zorgen voor een subtiel evenwicht. Vanaf 2003 tot en met de laatste praktijkproef '2b or not 2b' ziet men dat de vraagstelling in de studies en proeven steeds verder verwijderd raakt van zaken als prestaties en veiligheid, en zich in toenemende mate gaat richten op de praktische uitvoering. Het kernprobleem, dat om veiligheid draait, wordt steeds minder concreet betrokken bij het uitwerken van de plannen. Dan kan het gebeuren dat de praktische aspecten, waarvan we dachten dat we ze begrepen, op basis van niet-relevante of zelfs tegenstrijdige criteria worden ingericht. Daarbij ontstaat het risico dat de primaire doelstelling, in dit geval het veiliger maken van het aanvraag- en uitgifteproces, niet wordt gehaald.

Na 2005 neemt de divergentie tussen beleid en techniek significant toe. Centrale opslag wordt een randvoorwaarde en in de wet wordt opsporing en vervolging als additioneel doel vastgelegd. De gevolgen voor de techniek zijn groot en het vertrouwen dat wij erin leggen groeit evenredig. Want ondanks deze uitbreidingen worden er geen nieuwe studies of proeven gestart. Waren de uitdagingen rond de oorspronkelijke doelstelling al groot (namelijk de bestrijding van 'look alike fraude'), nu is de kloof nauwelijks meer te overbruggen. Wellicht besefte men dat ergens wel, maar was de belofte inmiddels te groot om terug te draaien.

En toch zal dat moeten. Zonder eerst een solide basis te hebben voor de meest fundamentele stap binnen het gehele biometrische proces, namelijk de afname en registratie van de biometrische gegevens, zal alles wat daar verder op wordt gebouwd wel eens onbetrouwbaar en inefficiënt kunnen worden. Slechte kwaliteit plaatjes kunnen de prestaties van een biometrische database voor jaren negatief beïnvloeden. Wanneer men daarvan doordrongen is, kan er maar één conclusie zijn: zonder serieuze investeringen

zullen we ons doel niet bereiken. Dus is een praktijkproef met een minimaal budget een gevaarlijke formule en zal het ontrekken van de feitelijke prestaties van het biometrische systeem (zoals kwaliteit en veiligheid) aan het zicht van het parlement alleen maar contraproductief werken. Het ontwikkelen van een goed biometrisch systeem vraagt om een heldere aanpak, een vaste koers en een diepgaand begrip van het kernprobleem en de techniek. Dat betekent dat de overheid bepaalde technische kennis absoluut in huis moet hebben, of tenminste moet weten waar deze is te vinden. Biometrie is geen simpel attribuut, maar een strategisch instrument, waarbij de strategische componenten diep begraven liggen in de kern van de technische werking ervan. De studies en proeven, met name vanaf 2003, geven er blijk van dat dat besef slechts in beperkte mate aanwezig was. Gerdien Keijzer-Baldé, sinds 1 april 2010 de directeur van het Agentschap BPR zegt over dit aspect:

> *"Neem allerlei vraagstukken op het terrein van biometrische gegevens. Ik moet, nu ik hier een halfjaar werk, constateren, dat wij geen eigen unit Research & Development hebben. Ja, er is één functionaris, en die is nu uitgeleend aan het programma reisdocumenten. Hier hebben we geen experts op het gebied van vingerafdrukken, iriscopie, etc. We moeten altijd externe deskundigen inhuren. Natuurlijk is het de vraag of je alles zelf in huis moet halen, maar je moet de kennis die ook elders is wel kunnen ontsluiten en er toegang tot hebben. Dat is belangrijk. Die kennis zit dus ook niet op het departement."*[89]

Het agentschap BPR heeft in de voorbereidingen van deze studie een uitnodiging voor een gesprek afgewezen. Het verzoek is doorverwezen naar de Directeur-Generaal van BZK. Op het moment van publicatie van deze studie was het verzoek nog in behandeling.

89 Interview B&R, oktober 2010.

## 11. Samenvatting en conclusies

### Het biometrische paspoort: techniek, beleid en politiek in Nederland

Als gevolg van de ICAO-standaard DOC9303 heeft de Europese Commissie de richtlijn EC2252/2004 uitgevaardigd. Deze schrijft het toevoegen van de chip aan het paspoort voor, inclusief het opslaan van een digitale afbeelding van het gezicht en twee vingers in de chip. Het doel daarvan is het bestrijden van 'look alike fraude'.

Binnen de Nederlandse politiek heeft er een verschuiving plaatsgevonden ten aanzien van deze oorspronkelijke functie die de biometrie moest vervullen. Vanaf circa 1999 tot circa 2004 was er uitsluitend sprake van het bestrijden van 'look alike' fraude, conform de Europese richtlijn. In alle parlementaire stukken wordt daar naar verwezen waneer het de omvang en legitimatie van de maatregel betreft. Vanaf 2004 ontstaat er een verschuiving naar centrale opslag en wordt de biometrische functionaliteit uitgebreid naar identiteitsfraude, opsporing, vervolging en terrorismebestrijding. Functioneel betekent dit dat er naast verificatie aan de hand van het paspoort (1:1) ook identificatie moet kunnen plaatsvinden (1:n).

### Techniek

Biometrie is de techniek waarbij aan de hand van fysieke lichaamskenmerken de identiteit van personen automatisch kan worden bepaald of geverifieerd. We spreken dan respectievelijk over identificatie en verificatie. Het eerste gebeurt aan de hand van een 1:n zoekactie aan de hand van uitsluitend de biometrische gegevens als zoekcriterium. Het tweede gebeurt nadat er een identiteitsclaim heeft plaatsgevonden (bijvoorbeeld door middel van een paspoort of id-kaart), op basis waarvan wordt gekeken of de biometrische gegevens bij de persoon horen die de identiteitsclaim heeft gedaan.

De kwaliteit en integriteit van de afgenomen vingerafdrukken en gezichtsopnames is van doorslaggevend belang voor de prestaties van het biometrische systeem als geheel (inclusief veiligheid). Dit is niet uitsluitend afhankelijk van de gekozen techniek: omgevingsfactoren, procedures en de vaardigheden van baliemedewerkers spelen een bijzonder grote rol. Training van baliemedewerkers is zo cruciaal dat certificering eigenlijk een vereiste zou moeten zijn.

Hoe groter het biometrische systeem, des te groter is de negatieve invloed van slechte biometrische images. Dat geldt in het bijzonder voor biometrische databases, waarbij 1:n zoekacties moeten plaatsvinden. De kwaliteitseisen voor een verificatiesysteem (1:1) kunnen aanzienlijk lager liggen dan voor een identificatiesysteem. Dat impliceert dat kwaliteitseisen voor een verificatiesysteem onbruikbaar zijn voor een identificatiesysteem. Het is dan ook onmogelijk om in een functioneel ontwerp over te stappen van verificatie naar identificatie, zonder drastische maatregelen te nemen ten aanzien van de criteria voor kwaliteit en betrouwbaarheid. Ook fall back scenario's dienen grondig te worden herzien wanneer wordt overgegaan op een identitificatiesysteem.

Hoe grootschaliger een identificatiesysteem, des te meer fouten er zullen optreden. Dit heeft grote gevolgen voor de inrichting van de processen en procedures. Een grootschalige test van NIST uit 2003 (NIST Fingerprint Vendor Technology Evaluation) heeft hierover een maatgevend rapport geschreven. In geen van de belangrijkste studies en rapporten die zijn uitgevoerd door of in opdracht van de Nederlandse overheid in die periode of daarna wordt naar deze test verwezen.

De vele factoren maken biometrie tot een complexe materie. Het risico bestaat dat de problematiek wordt vereenvoudigd om het in brede kring bespreekbaar te maken en besluitvorming te versnellen. Daardoor kan ten onrechte een te positief of te negatief beeld ontstaan. Biometrie wordt dan snel een speelbal van politieke discussies en agenda's.

**De industrie**

Binnen justitiële organisaties wordt biometrie binnen en buiten Nederland al gedurende vele jaren intensief gebruikt voor opsporing en vervolging. Doordat deze toepassingen altijd binnen een nationale context vallen (elk land is verantwoordelijk voor zijn eigen criminele database), is er wereldwijd een nationale verkaveling van de biometriemarkt te zien. Daarbij voorziet slechts een beperkt aantal (circa vier) aanbieders de wereldmarkt. Hoewel het aantal toepassingsgebieden zich gestaag uitbreidt, zijn het nog steeds deze aanbieders die de markt domineren. Door een gebrek aan volwassen standaards zijn de

marktleiders in de gelegenheid om hun nationale markten veilig te stellen door hun technologie onderling niet uitwisselbaar te maken, zonder dat daarvoor grote investeringen nodig zijn. Interoperabiliteit is in de biometrie dus geen vanzelfsprekendheid. Dat zorgt ervoor dat de producten van verschillende leveranciers moeilijk met elkaar zijn te vergelijken en dat geclaimde prestaties van hun producten slecht kunnen worden geverifieerd. Als leveranciers van biometrische producten daarbij ook end-to-end solutions op de markt brengen (bijv. biometriebedrijf Morpho dat ook paspoorten met de bijbehorende infrastructuur levert) is het voor de klant vrijwel onontkoombaar om in een 'vendor lock in' terecht te komen.

Er zijn (inmiddels) standaards, maar er zijn nog niet voldoende tests en testcapaciteiten om de conformiteit van biometrische producten onafhankelijk te laten evalueren. Het gevolg is dat klanten zelf de producten gaan testen, meestal aan de hand van een benchmark in de context van de beoogde toepassing. Dat vereist echter veel technische kennis, een onafhankelijke en nuchtere blik op de problematiek en duidelijke test criteria. Met politieke ambities en besluitvorming als grondslag kan dit voor overheden een grote uitdaging zijn, omdat wetenschappelijke objectiviteit makkelijk kan wijken voor politiek opportunisme.

Soms wordt het verwijt gemaakt dat de industrie haar producten te veel opdringt en daarbij de prestaties en mogelijkheden van de techniek te mooi afschildert. Maar vaak is de klant daar zelf mede schuldig aan, bijvoorbeeld doordat de technische oplossing politiek is gedreven. In dat geval worden de claims van de industrie maar wat graag overgenomen. Of omdat de klant zelf niet weet welke eisen hij aan de techniek moet stellen en niet goed in staat is om de claims van de industrie onafhankelijk te testen. Het is daarom essentiëel dat voor grootschalige en kritische projecten zoals het biometrische paspoort onafhankelijke testinstituten en erkende expertisecentra (zoals TNO en NFI) structureel worden ingezet bij het opstellen, uitvoeren en evalueren van tests en pilots, en dat er wordt geïnvesteerd in duurzame kennis.

**Voorbereidende studies en proeven niet (voldoende) relevant voor huidige Paspoortwet**

Tussen 1999 en 2005 zijn er diverse haalbaarheidsstudies en proeven uitgevoerd. Deze waren gebaseerd op het opslaan van de biometrie uitsluitend in de chip van het paspoort, wat later ook het uitgangspunt van de Europese richtlijn zou zijn. In 2003 wordt decentrale opslag voorgesteld, uitsluitend om op basis van verificatie (1:1) van de biometrische gegevens onbedoelde fouten en opzettelijke fraude bij het aanvraag- en uitgifteproces te voorkomen. Hierover een aantal observaties.

- De proeven uit 2001 waren te kleinschalig en niet representatief voor het beoogde gebruik.
- Rond de proef '2b or not 2b' bestaat een aantal onduidelijkheden. Er is getracht verschillende leveranciers van biometrische apparatuur met elkaar te vergelijken, terwijl hun techniek niet interoperabel is. Zo waren er zeker in die tijd verschillende opvattingen tussen de leveranciers over de kwaliteit van de afgenomen vingerafdrukken en over de plaatsing van de minutiae. Gedurende de proef zijn de drempelwaarden aangepast. Dit was volgens het NFI niet goed gedocumenteerd. Onduidelijk is welke invloed dat op de betrouwbaarheid heeft gehad. Het NFI is achteraf gevraagd om hun interpretatie van de testdata te geven, maar beweert dat "er geen chocola van te maken was". Veel uitkomsten moesten achteraf worden geïnterpreteerd op basis van geschatte drempelwaarden. De uitkomsten van '2b or not 2b' zijn door de overheid gebruikt als basis voor de besluitvorming.
- Het marktonderzoek uit 2003 naar de kennis en houding van de burgers met betrekking tot de toepassing van biometrie in het paspoort is slechts beperkt bruikbaar omdat volgens het kwalitatieve deel van het onderzoek de burgers geen idee hebben wat de techniek behelst. Het marktonderzoek ging uit van de opslag van de biometrische gegevens in het paspoort. Omdat sinds circa 2004 sprake is van centrale opslag en ook het gebruik van de biometrische data was uitgebreid, is het onderzoek op dat punt achterhaald. Het is niet bekend of er naar aanleiding van die wijzigingen een nieuw onderzoek naar de acceptatie is gedaan.

**Focus op het proces, veiligheid secundair**

Bij de proeven en studies hebben processen centraal gestaan. De veiligheid heeft een ondergeschikte rol gespeeld. Er is voornamelijk gekeken hoe de biometrie zo eenvoudig mogelijk aan de bestaande processen en procedures kon worden toegevoegd. Er is

beperkt aandacht besteed aan de vraag of en in hoeverre de biometrie het centrale probleem oplost. Het toevoegen van biometrie aan het Nederlandse paspoort en identiteitssysteem is voornamelijk als een administratieve handeling behandeld. Daardoor ontstaan er risco's, waaronder:

- Een inefficiënt systeem vanwege lage prestaties (hoge kosten).
- Identiteitsfraude vanwege een manipuleerbaar registratieproces (fraude).
- Rechtszaken vanwege systeemfouten (maatschappelijke verontwaardiging).

**Gebrek aan heldere doelstellingen en criteria voor succes**

Haalbaarheidsstudies vragen om duidelijke doelstellingen en criteria voor de prestaties en de veiligheid. Als de doelstellingen niet helder staan beschreven, is een grondige haalbaarheidsstudie niet mogelijk. De vraag of met biometrie de vooraf gestelde doelstellingen in de gegeven context haalbaar zijn (en zo ja: hoe), is niet helder gesteld en dus ook niet duidelijk beantwoord. Als wordt gesteld dat 'voor een effectief gebruik van biometrie centrale opslag randvoorwaardelijk is', dan zou een goede technische onderbouwing op zijn plaats zijn.

**Verantwoordelijk agentschap weinig communicatief en te weinig technisch onderlegd**

Het agentschap BPR lijkt in dit gehele traject een weinig communicatieve rol te hebben gespeeld. Kritische meningen kregen niet altijd de ruimte die zij wellicht verdienden. Erkende specialisten lijken niet in alle voorbereidingen voldoende te zijn betrokken (zoals bv. het NFI en TNO). De kans bestaat dan dat gebrek aan inhoudelijke technische kennis bijgedraagt aan onderschatting van de complexiteit van de biometrische technologie.

**Probleemstelling niet helder**

Het belangrijkste bezwaar van de proeven en studies die zijn uitgevoerd, is dat er vooraf geen heldere probleemstelling is geformuleerd op het gebied van veiligheid en betrouwbaarheid. Ongetwijfeld houdt dat verband met het feit dat het onduidelijk was:

- welk probleem het precies moest gaan oplossen;
- hoe groot het vermeende probleem is;

- in welke mate men verwacht dat biometrie daar een oplossing voor kan/moet bieden.

Identiteitsfraude en terrorismebestrijding zijn brede begrippen met allerlei verschijningsvormen, waarvan 'look alike fraude' er slechts één is. Niet duidelijk is wat en hoe groot de bijdrage van biometrie precies moet zijn voor welke vorm(en) van identiteitsfraude.

**Proportionaliteit niet aangetoond**

De verantwoordelijke bewindslieden hebben gesteld dat de maatregelen zoals beschreven in de nieuwe Paspoortwet proportioneel zijn en de inbreuk op de private levenssfeer van de burgers rechtvaardigen. Dit is echter door geen enkele studie, rapport of test helder onderbouwd op basis van kwantificeerbare en verifiëerbare afwegingen. Het CBP onderschrijft dit in haar advies van maart 2007.

**Nederland gaat verder dan Europa en neemt daarmee risico's**

Nederland gaat verder dan de Europese Commissie voorschrijft, wellicht vanuit de ambitie om, net zoals bij het succesvolle nieuwe paspoort, ook op het gebied van de biometrie een vooraanstaande rol te spelen in Europa. In plaats van het creëren van duidelijkheid omtrent de techniek en functie van het biometrische paspoort in de context van de Europese richtlijn, zijn de functionaliteit, complexiteit en de daardoor ontstane risico's uitgebreid. Immers, de standaardisatie in de biometrie is allerminst voltooid en ervaring met nationale uitrol van biometrie is er evenmin. Hoewel de biometrische apparatuur in de loop der jaren sterk is verbeterd, zijn de omstreeks 2000-2004 reeds bekende uitdagingen rond grootschalige toepassingen van biometrie (zie bijvoorbeeld de test van NIST uit 2003, maar ook *Alle mensen zijn Ongelijk* van TNO uit 1999) niet verdwenen. Alle zorgen rond de prestaties en veiligheid bestaan nog steeds. Het CBP heeft in 2007 al gewezen op de risico's en de beperkte onderbouwing van de plannen door een kritisch rapport te publiceren (zie www.cbpweb.nl).

**Slotvraag**

Tussen de eerste verkenningen rond het potentiële gebruik van biometrie in 1999 en de uiteindelijke wetgeving en ingebruikname van de vingerafdrukapparatuur in 2009, heeft

het Programma van Eisen ten aanzien van het biometrische paspoort een aantal wijzigingen ondergaan. De technische verantwoording daarvoor ontbreekt. Er zijn naar aanleiding van de wijzigingen geen nieuwe haalbaarheidstudies, proeven of onderzoeken gedaan. De vraag is hoe in dit stadium bepaald gaat worden of we met de Paspoortwet op de goede weg zijn: is het effectief, is het de investering waard en is de inbreuk op de privacy van burgers inderdaad gerechtvaardigd.

***Max Snijder, november 2010***

## 12. Literatuurlijst

*Documenten*[90]*:*


Atos (2005) UK Passport Service Biometrics Enrollment Trial Report , Atos Origin May 2005
http://hornbeam.cs.ucl.ac.uk/hcs/teaching/GA10/lec3extra/UKPSBiometrics_Enrolment_Trial_Report.pdf

Bausinger, O. and Seidel, U. (2007), *Next generation e-Passport fingerprint enrolment – quality vs. time.*
http://www.itl.nist.gov/iad/894.03/quality/workshop07/proc/Bausinger_Seidel_v10.pdf

Böhre, V. (2010) *Happy landings? Het biometrische paspoort als zwarte doos*, Den Haag, Wetenschappelijke Raad voor het Regeringsbeleid, www.wrr.nl.

BPR (2003), *Onderzoek naar de toepassing van biometrische kenmerken voor Nederlandse reisdocumenten*, Den Haag, 6 juni 2003, Project Biometrie, Agentschap BPR.

BZK (2005), *Evaluatierapport Biometrieproef 2b or not 2b*, Ministrie van Binnenlandse Zaken en Koninkrijksrelaties (BZK), Amsterdam 2005.
http://www.cartidownload.ro/Diverse/463554/Evaluatierapport_2b_or_Not_2b

Council Regulation (EC) No 2725/2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention (11 December 2000)


90 Webpagina's laatst bezocht op 25 november 2010.

Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States (13 December 2004)

Council Regulation (EC) No 512/2004 Establishing the Visa Information System (VIS) (8 June 2004).

Council document 5733/07 (2007) Need for systematic use of biometrics in checks at external borders.

European Data Protection Supervisor: Opinion of the European Data Protection Supervisor on the modified proposal for a Council Regulation amending Regulation (EC) 1030/2002 laying down a uniform format for residence permits for third-country nationals. OJ 2006/C 320/10.

Feng J. and Jain, A. K. (2010), *Fingerprint Reconstruction: From Minutiae to Phase,*IEEE Transactions on Pattern Analysis and Machine Intelligence, 2010. http://www.computer.org/portal/web/csdl/doi/10.1109/TPAMI.2010.77

Grother, P. (2004) *Face Recognition Vendor Test 2002 Supplemental Report,* NIST IR7083, National Institute of Standards & Technology, Gaithersburg Maryland, February 2004. http://www.frvt.com/DLs/frvt2002_supplemental.pdf

NIST (2008), *Usability and Biometrics: Ensuring successful biometric systems* http://zing.ncsl.nist.gov/biousa/docs/Usability_and_Biometrics_final2.pdf

NIST(2007), *FRVT 2006 and ICE 2006 Large-Scale Results*, NIST IR7408.

NIST (2002) *Use of Technology Standards and Interoperable Databases with Machine-Readable, Tamper-Resistant Travel Documents – Appendix A*, November 2002. http://www.itl.nist.gov/iaui/894.03/fing/fing.html

Phillips, P. J., Grother, P., Micheals, R. J., Blackburn, D. M., Tabassi, E. and

Bone, M., *Face recognition vendor test 2002,* NIST IR 6965, National Institute of Standards & Technology, Gaithersburg Maryland, March 2003.

Van Renesse, R. (2002), *Implications of ApplyingBiometrics for Travel Documents*, SPIE Conference on Optical Security and Counterfeit Deterrence Techniques IV, Vol. 4677, San Jose, CA, January 23-25, 2002, pp. 290-298 (www.vanrenesse-consulting.com/index.php?page=paper.htm)

Van Renesse, R. (2002) *Implications of Biometrics for Travel Documents*, 5th International Conference on Fraudulent Documents, Amsterdam 11 april 2002 (www.vanrenesse-consulting.com/index.php?page=paper.htm)

Theofanos, M. et al. (2008), *Assessing face acquisition*, NISTIR 7540, http://zing.ncsl.nist.gov/biousa/docs/face_IR-7540.pdf

Theofanos, M. et al. (2006), *Effects of scanner height on fingerprint capture*, NISTIR 7382.
http://zing.ncsl.nist.gov/biousa/docs/NISTIR_7382_Height_Study.pdf

Theofanos, M. et al. (2008), *Usability Testing of Height and Angles of Ten-Print Fingerprint Capture,* NISTIR 7504
http://zing.ncsl.nist.gov/biousa/docs/NISTIR-7504%20height%20angle.pdf

TNO (1999), Van Renesse, R., *Quick Scan Biometrie: Alle Mensen zijn Ongelijk*, in opdracht van BPR.

107th United States Congress (2002), Enhanced Border Security and Visa Entry Reform Act, Public Law 107-173, Washington D.C., 14 May 2002.

107th United States Congress (2001), USA PATRIOT ACT, Public Law 107-56, Washington D.C., 26 October 2001.

Veldkamp (2003), Verkennend Onderzoek Biometrie (kenmerk BPR2003/53281).

VKA/TNO (2002) Biometrics Against Look Alike Fraud (kenmerk BPR2002/100783).

Wilson, C., Hicklin, R. A., Korves, H., Ulery, B., Zoepfl, M., Bone, M., Grother, P., Micheals, R., Otto, S. and Watson, C. (2003) *Fingerprint Vendor Technology Evaluation 2003 Analysis Report*. http://fpvte.nist.gov/report/ir_7123_summary.pdf

Wood, Stephen S. and Wilson, Charles L. (2004) *Studies of Plain-to-Rolled Fingerprint Matching Using the NIST Algorithmic Test Bed (ATB)*, NIST IR7112, April 2004; National Institute of Standards & Technology, Gaithersburg Maryland. ftp://sequoyah.nist.gov/pub/nist_internal_reports/ir_7112.pdf

Wilson, C. L., Garris, M. D. and Watson, C. A. (2004) *Matching Performance for the US-VISIT IDENT SystemUsing Flat Fingerprints*,NISTIRIR7110 National Institute of Standards & Technology, Gaithersburg Maryland. http://www.nist.gov/manuscript-publication-search.cfm?pub_id=151587

Wilson C., Watson C., Garris, Hicklin, A. (2003) *Studies of Fingerprint Matching Using the NIST Verification Test Bed (VTB)*, NISTIR 7020, 7 July 2003. ftp://sequoyah.nist.gov/pub/nist_internal_reports/ir_7020.pdf

Watson, C., Wilson, C.,Marshall, K., Indovina, M. and Snelick, R. (2005) *Studies of One-to-One Fingerprint Matching with Vendor SDK Matchers*, NISTIR 7221, National Institute of Standards & Technology, Gaithersburg Maryland. http://www.nist.gov/customcf/get_pdf.cfm?pub_id=151593

**Geraadpleegde Websites**


http://www.european-accreditation.org
http://www.iso.org
http://www.nist.gov
http://www.nationalbiometrics.org
http://www.bionbiometrics.com
http://www.biometricgroup.com
http://www.commoncriteriaportal.org
http://www.ce-marking.org/what-is-ce-marking.html
http://identityproject.lse.ac.uk/identityreport.pdf
http://www.itl.nist.gov/ANSIASD/
http://www.fbi.gov/hq/cjisd/iafis/cert.htm
http://www.cen.eu/cen/Sectors/Sectors/ISSS/Focus/Pages/Biometrics_FG.aspx
http://biotestingeurope.eu
http://www.mtitproject.com
http://www.eubiometricsforum.com
http://findbiometrics.com
http://www.biometricscatalog.org
http://www.epass.de/
http://ww.bsi.de/
http://www.iso.org/iso/iso_technical_committee.html?commid=313770
www2.icao.int/EN/MRTD/Pages/Downloads.aspx

## 13. Lijst met afkortingen

| | |
|---|---|
| AFIS | Automated Fingerprint Identification System |
| ANSI | Amarican National Standards Institute |
| ATM | Automated Teller Machine |
| BAC | Basic Access Control |
| BIG | Brussels Interoperability Group |
| BioAPI | Biometric Application Programming Interface |
| BIT | Beleid, Informatie en Technologie |
| BMS | Biometric Matching System |
| BPR | Basisregistratie Persoonsgegevens en Reisdocumenten |
| CBP | College Bescherming Persoonsgegevens |
| CBEFF | Common Biometric Exchange Formats Framework |
| CQAR | Central Quality Assurance Repository |
| DRIVeS | Dynamisch Reisdocumenten Informatie- en Verificatie Systeem |
| EAC | Extend Access Control |
| EC | European Community |
| EG | Europese Gemeenschap |
| FAR | False Accept Rate |
| FIPS | Federal Information Processing Standard |
| FMR | False Match Rate |
| FNMR | False Non-Match Rate |
| FpVTE | NIST Vendor Fingerprint Technology Evaluation |
| FRR | False Reject Rate |
| FTA | Failure To Acquire |
| FTE | Failure To Enrol |
| GBA | Gemeentelijke basisadministratie persoonsgegevens |
| ICAO | International Civil Aviation Organization |
| ICT | Informatie en Communicatie Technologie |
| IEC | International Electronic Commission |
| ISO | International Organization for Standardization |

| | |
|---|---|
| IUID | Indian Unique Identity |
| JMCE | Jean Monnet Center of Excellence |
| MINEX | Minutiae Interoperabiliteit Exchange Test |
| MTIT | Minutiae Template Interoperability Testing |
| NGR | Nieuwe Generatie Reisdocumenten |
| NFI | Nederlands Forensisch Instituut |
| NFIQ | NIST Fingerprint Image Quality |
| NIST | National Institute for Standards and Technology |
| NVVB | Nederlandse Vereniging Voor Burgerzaken |
| OM | Openbaar Ministerie |
| ORRA | Online Raadpleegbare Reisdocumenten Administratie |
| PIV | Personal Identity Verification |
| PKD | Public Key Directory |
| PKI | Public Key Infrastructure |
| PvE | Programma van Eisen |
| RAAS | Gemeentelijk station voor invoer en opslag van persoonsgegevens |
| RAPID | Automatic Identification of Passengers Holding Travelling Documents (Portugal) |
| SLA | Service Level Agreement |
| SIS | Schengen Informatie Systeem |
| TILT | Tilburg Institute for Law, Technology and Society |
| TAR | True Accept Rate |
| TRR | True Reject Rate |
| UIDAI | Unique Identification Authority of India |
| US-VISIT | U.S. Visitor and Immigrant Status Indicator Technology |
| VDM | Vendor Device Manager |
| VIS | Visa Information System |
| Wbp | Wet bescherming persoonsgegevens |
| WRR | Wetenschappelijke Raad voor het Regeringsbeleid |

## NOTEN

1 De eerste generatie nieuwe reisdocumenten werd in 2001 geleverd door Enschedé-Sdu, een 50-50 joint venture van Joh.Enschedé en SDU Uitgevers. In de loop van 2003 valt deze joint venture uit elkaar en neemt SDU de aandelen van Joh.Enschedé over. Het bedrijf het nu SDU Identification en is 100% eigendom van de staat. Een aantal jaren later wordt het gehele uitgevers bedrijf verkocht aan een consortium van ABN-AMRO en Allianz. SDU Identification wordt daarna in juni 2008 verkocht aan het toenmalige Sagem Sécurité, onderdeel van het Franse Safran Group, dat voor 30% eigendom is van de Franse overheid.. SDU Identification krijgt de naam Sagem Identification. De naam Sagem is inmiddels omgedoopt in Morpho.