NGR99/90565

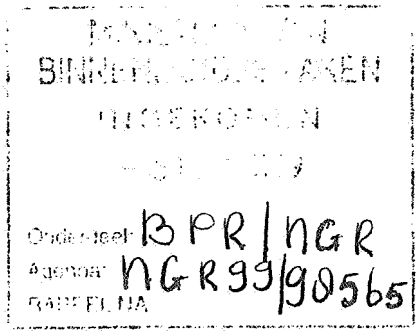
TNO Centrum voor Evaluatie van Instrumentatie
en Beveiligingstechniek (EIB)

Stieltjesweg 1
Postbus 5013
2600 GA Delft

Telefoon 015 269 20 00
Fax 015 269 21 11

clep sup
17/11/2000
PK

Per koerier:
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Project Nieuwe Generatie Reisdocumenten
[redacted]
Postbus 10451
2501 HL 's-GRAVENHAGE



Doorkiesnummer
015[redacted]

Datum
3 december 1999

Nummer
EIB-LTR-990321

Uw brief

Projectnummer
01321.01.01

Onderwerp
Project Quick Scan Biometrie

Geachte[redacted]

Bijgaand zenden wij u een exemplaar van rapport nr. EIB-RPT-990069, d.d. 29 oktober 1999, getiteld "Quick Scan Biometrie - alle mensen zijn ongelijk !".

Tevens sluiten wij een concept-factuur in betreffende de laatste termijn van dit project bij.

Wij vertrouwen u hiermede van dienst te zijn.

Hoogachtend,

[redacted]
secretaresse

Bijlagen:

Kopie: DS-FEZ-EIB, Ir H. Buitenhuis, R.L. van Renesse, -RTW/jdb

Het EIB heeft fysiek en organisatorisch een neutrale, onafhankelijke positie binnen TNO Technisch Physische Dienst TU Delft (TPD).

Het EIB vervult opdrachten tot het ontwikkelen en toepassen van standaarden, evaluatiecriteria, -procedures, -methoden en -technieken voor een breed scala van systemen en produkten.

TNO-rapport
EIB-RPT-990069

Quick Scan Biometrie - alle mensen zijn ongelijk !

TNO Centrum voor Evaluatie
van Instrumentatie
en Beveiligingstechniek (EIB)

Stieltjesweg 1
Postbus 5013
2600 GA Delft

Telefoon 015 269 20 00
Fax 015 269 21 11

Datum
29 oktober 1999

Auteur(s)
[redacted]

Gecontroleerd door
[redacted]

Goedgekeurd door
[redacted]

Projectnummer
01321/01.01

Aan

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
's-Gravenhage

Quick Scan Biometrie:
Alle mensen zijn ongelijk

Biometrie is de automatische bepaling van de identiteit van een levend individu door het meten van een uniek fysiek kenmerk of gedragskenmerk

Inhoud

Samenvatting

Het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) verwacht dat alle reisdocumenten (paspoort en ID-kaart), met uitzondering van de nooddocumenten, in de toekomst zullen worden voorzien van een mogelijkheid tot biometrische verificatie van de identiteit van de houder. Met behulp van biometrische controle kan worden vastgesteld of de aanbieder van het document de legitieme houder daarvan is.
BZK doet met het oog op deze ontwikkeling een onderzoek naar de bruikbaarheid van biometrie in twee door haar onderscheiden groepen van toepassingsgebieden: (1) het onderkennen van 'look-alikes' (dubbelgangers) bij de controle van reisdocumenten en (2) het gebruik van reisdocumenten als identiteitsbewijs voor elektronische identificatie op afstand. Dit laatste toepassingsgebied kan worden gesplitst in de toepassingsgebieden 'biometrische kiosk in openbare ruimtes' en 'PC in de privé sfeer'.

Het doel van dit onderzoek is het beantwoorden van de vraag welke biometrische techniek of technieken ingezet kunnen worden in deze drie onderscheiden toepassingsgebieden. Om deze vraag te kunnen beantwoorden zijn beoordelingscriteria opgesteld, waarmee de verschillende beschikbare biometrische technieken kunnen worden beoordeeld op hun geschiktheid voor het toepassingsgebied.
Het onderzoek is in drie fasen uitgevoerd:

1. Vaststellen van de beoordelingscriteria.
2. Vraaggesprekken met deskundigen ter zake.
3. Inventarisatie van biometrische technieken en selectie overeenkomstig de beoordelingscriteria.

Tevens heeft het onderzoek tot doel gehad vast te stellen wat de kritische succesfactoren zijn voor toepassing van biometrie op zeer grote schaal voor zeer heterogene gebruikersgroepen.

Vastgesteld is dat - in de genoemde toepassingsgebieden - 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.

Vastgesteld is tevens dat de drie toepassinggebieden kunnen worden onderscheiden op de mate van begeleiding en daaruit volgend in de mate van vereiste beveiliging:

Toepassing	Vorm	Vereiste beveiligingsniveau
'Look-alikes'	begeleid	Laag
Kiosk in openbare ruimte	semi-begeleid	Gemiddeld
PC in privé sfeer	niet begeleid	Hoog

Op grond van dit onderscheid in beveiligingsniveau zijn - voor de onderscheiden toepassingsgebieden - voorlopige foutpercentages gespecificeerd voor de 'false reject rate' (FRR) en de 'false accept rate' (FAR) van de toe te passen biometrische technieken. De failure to enrol (FTE) is pro memorie vermeld.

Type fout	'Look-alikes'	Publieke kiosk	Privé PC
FRR	5%	0,5%	0,05%
FAR	0,1%	0,01%	0,001%
FTE	p.m.	p.m.	p.m.

Zeer grootschalige, operationele toepassingen van biometrie bestaan momenteel nog niet. Uit de literatuur (appendix III) en een beschouwing betreffende de betrouwbaarheid van voor biometrische apparatuur gespecificeerde foutpercentages bij zeer grootschalige toepassingen met zeer heterogene gebruikersgroepen, komt naar voren dat deze percentages veelmeer gegeven worden door het psychologische profiel van de gebruikersgroep dan door de specifieke, technische apparaateigenschappen. Onafhankelijk van de biometrische techniek mag een FRR tussen ruwweg 1% en 5% worden verwacht voor zeer grootschalige toepassingen met zeer heterogene gebruikersgroepen.
Hieruit volgt de verwachting dat de toepassing van biometrie in het toepassingsgebied privé PC niet eenvoudig gerealiseerd kan worden.

De ten behoeve van de selectie vastgestelde beoordelingscriteria zijn:
- weerstand tegen vandalisme
- maatschappelijke acceptatie
- eigenschappen van het biometrische kenmerk
- betrouwbaarheid en 'proven technology'
- eigenschappen en gebruik van de biometrische apparatuur

De FRR blijkt vooralsnog geen betrouwbaar beoordelingscriterium voor biometrische technieken. Ook over de FAR van biometrische technieken is te weinig bekend om deze als objectief en betrouwbaar beoordelingscriterium te accepteren voor het onderling vergelijken van biometrische technieken.

Op grond van de vereiste commerciële beschikbaarheid komen een vijftal biometrische technieken voor nadere beschouwing in aanmerking:
- gezichtsherkenning
- irisherkenning
- vingerpatroonherkenning
- stemherkenning
- dynamische handtekening

Op grond van de bovengenoemde beoordelingscriteria zijn vervolgens drie biometrische technieken geselecteerd die het beste kunnen worden ingezet voor de verschillende toepassingsgebieden:

biometrie	**'look-alikes'**	**publieke kiosk**	**privé PC**
Gezichtsherkenning	o	o	o
Irisherkenning	o	•	
Vingerpatroonherkenning			•

- • positieve score op alle beoordelingscriteria
- o positieve score op een belangrijk deel van de beoordelingscriteria

Ieder van de beoordelingen heeft een zo zorgvuldig mogelijke weging plaatsgevonden van de biometrische technieken tegen de vastgestelde beoordelingscriteria. Het eindresultaat van al deze wegingen is schematisch en zal er anders uitzien wanneer de verschillende criteria anders worden gewogen. Dit resultaat kan daarom niet worden beoordeeld zonder de toelichtingen op de verschillende wegingen in aanmerking te nemen.

Zeer grootschalige, operationele toepassingen van biometrie bestaan momenteel nog niet. Uit de literatuur (appendix III) en een beschouwing betreffende de betrouwbaarheid van voor biometrische apparatuur gespecificeerde foutpercentages bij zeer grootschalige toepassingen met zeer heterogene gebruikersgroepen, komt naar voren dat deze percentages veelmeer gegeven worden door het psychologische profiel van de gebruikersgroep dan door de specifieke, technische apparaateigenschappen. Onafhankelijk van de biometrische techniek mag een FRR tussen ruwweg 1% en 5% worden verwacht voor zeer grootschalige toepassingen met zeer heterogene gebruikersgroepen.
Hieruit volgt de verwachting dat de toepassing van biometrie in het toepassingsgebied privé PC niet eenvoudig gerealiseerd kan worden.

De ten behoeve van de selectie vastgestelde beoordelingscriteria zijn:
- weerstand tegen vandalisme
- maatschappelijke acceptatie
- eigenschappen van het biometrische kenmerk
- betrouwbaarheid en 'proven technology'
- eigenschappen en gebruik van de biometrische apparatuur

De FRR blijkt vooralsnog geen betrouwbaar beoordelingscriterium voor biometrische technieken. Ook over de FAR van biometrische technieken is te weinig bekend om deze als objectief en betrouwbaar beoordelingscriterium te accepteren voor het onderling vergelijken van biometrische technieken.

Op grond van de vereiste commerciële beschikbaarheid komen een vijftal biometrische technieken voor nadere beschouwing in aanmerking:
- gezichtsherkenning
- irisherkenning
- vingerpatroonherkenning
- stemherkenning
- dynamische handtekening

Op grond van de bovengenoemde beoordelingscriteria zijn vervolgens drie biometrische technieken geselecteerd die het beste kunnen worden ingezet voor de verschillende toepassingsgebieden:

biometrie	**'look-alikes'**	**publieke kiosk**	**privé PC**
Gezichtsherkenning	o	o	o
Irisherkenning	o	•	
Vingerpatroonherkenning			•

- • positieve score op alle beoordelingscriteria
- o positieve score op een belangrijk deel van de beoordelingscriteria

Ieder van de beoordelingen heeft een zo zorgvuldig mogelijke weging plaatsgevonden van de biometrische technieken tegen de vastgestelde beoordelingscriteria. Het eindresultaat van al deze wegingen is schematisch en zal er anders uitzien wanneer de verschillende criteria anders worden gewogen. Dit resultaat kan daarom niet worden beoordeeld zonder de toelichtingen op de verschillende wegingen in aanmerking te nemen.

Kritische succesfactoren zijn geformuleerd voor de toepassing van biometrie op zeer grote schaal met zeer heterogene gebruikersgroepen. Deze kritische succesfactoren omvatten de organisatie, de acceptatie door de gebruiker, de betrouwbaarheid van de techniek en de technologie.

Tenslotte zijn aanbevelingen gedaan m.b.t. het aanscherpen van de beoordelingscriteria, geënt op een meer gedetailleerde beschrijving van de toepassingsgebieden, voor nader onderzoek naar het combineren van biometrische technieken, de ontwikkeling van APIs, de toepassing van public key infrastructures, en het volgen van de ontwikkelingen op het gebied van grootschalige toepassingen van biometrie.

1 Inleiding

1.1 Probleemstelling

Het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) verwacht dat alle reisdocumenten (paspoort en ID-kaart), met uitzondering van de nooddocumenten, in de toekomst zullen worden voorzien van een mogelijkheid tot biometrische verificatie van de identiteit van de houder. Biometrische controle kan in hoge mate bijdragen tot het vaststellen of de aanbieder van het document de legitieme houder ervan is. BZK doet met het oog op deze ontwikkeling een onderzoek naar de bruikbaarheid van biometrie in twee door haar onderscheiden groepen van toepassingsgebieden: (1) het onderkennen van 'look-alikes' (dubbelgangers) bij de controle van reisdocumenten en (2) het gebruik van reisdocumenten als identiteitsbewijs voor elektronische identificatie op afstand. Beide toepassingsgebieden worden door BZK als even belangrijk gezien.

1. **Het onderkennen van 'look-alikes' bij de controle van reisdocumenten.**
   Het 'look-alike' probleem treedt op wanneer een overtuigende verificatie van de identiteit van de houder niet kan geschieden op basis van de pasfoto in het reisdocument. Dit is het geval als het reisdocument wordt aangeboden door een niet rechtmatige houder die min of meer sterk gelijkt op de rechtmatige houder. Deze situatie speelt zich in eerste instantie af op een beperkt aantal punten: luchthavens en mobiele grenscontrole in een relatief gesloten groep (reizigers).

   Het misbruik van documenten door 'look-alikes' is echter niet alleen vastgesteld bij grenscontrole, maar eveneens bij de dienstverlening door de gemeenten. Wanneer het 'look-alike' probleem in dat bredere verband wordt gezien, ontstaat een nieuw toepassingsgebied voor een grote, open en heterogene groep burgers met controle op een groot aantal punten.

   Kenmerkend voor dit toepassingsgebied is dat de aanbieder persoonlijk aanwezig is om het reisdocument voor controle aan de ambtenaar te overhandigen. Dit laat de mogelijkheid open om, zonder gebruik te maken van biometrie, een persoons-authenticatie uit te voeren op basis van een vergelijking van de gezichtskenmerken van de aanbieder met die op de pasfoto. Eerst wanneer deze vergelijking tot twijfel leidt, ontstaat de noodzaak een biometrische authenticatie uit te voeren. De biometrische authenticatie berust dan op een selectie van twijfelgevallen. Daar de controle in alle gevallen plaatsvindt onder begeleiding van een aanwezige ambtenaar, behoeft het niveau van beveiliging slechts relatief laag te zijn.

2. **Het gebruik van het reisdocument als identiteitsbewijs voor elektronische identificatie op afstand.**
   Het reisdocument biedt, naast de mogelijkheid tot grensoverschrijding, een meer algemene functionaliteit als identificatiedocument. In het verlengde hiervan wordt door BZK de mogelijkheid onderzocht van de toepassing van biometrie voor verificatie t.b.v. zogenaamde elektronische dienstverlening door de overheid op afstand. Hierbij wordt gedacht aan het aanvragen van een uittreksel uit het bevolkingsregister, verlengen van het rijbewijs, het regelen van een uitkering, zelfs aan "elektronisch stemmen" op afstand wordt gedacht [1]. Ook wordt gedacht aan de toepassing van biometrie t.b.v. de grenscontrole van regelmatige reizigers, waardoor de grenscontrole van deze groep reizigers automatisch en sneller kan verlopen.

Hier is sprake van een veelheid van toepassingsgebieden, die ieder op zich beoordeeld moeten worden op de onderscheiden eisen die deze met zich meebrengen.
Het reisdocument zal voor deze dienstverlening op afstand, naast biometrie ook gebruik maken van versleutelings-technieken die gebruikt worden voor de card-authenticatie. Door toepassing van biometrie kan identiteitsfraude naar verwachting grotendeels worden voorkomen.
Deze toepassing, ten behoeve van dienstverlening op afstand door de overheid, betreft een brede, open omgeving waarin diverse elektronische diensten worden geboden aan een zeer grote, heterogene groep burgers met controle op een groot aantal punten.

Kenmerkend voor dit tweede toepassingsgebied is dat het authenticatie-proces niet begeleid is, de controle is automatisch, op afstand en zonder direct toezicht van een ambtenaar. Persoons-authenticatie dient dus in alle gevallen te worden uitgevoerd op basis van biometrie. Twee situaties kunnen hierbij worden onderscheiden: biometrische apparatuur in publieke ruimtes en in de privé sfeer (PC thuis).

1. Biometrische apparatuur in publieke ruimtes
De biometrische apparatuur is voor het publiek algemeen toegankelijk, bijvoorbeeld in de vorm van een automatische kiosk in een publieke ruimte, niet permanent bewaakt, maar wel min of meer in het zicht van personeel. Hier kan van een semi-begeleide toepassing worden gesproken, waarbij een gemiddelde beveiliging op zijn plaats is.

2. Privé biometrische apparatuur
Voor biometrische apparatuur verbonden met bijvoorbeeld een PC in de privé sfeer of in kantoorruimtes is van enige begeleiding geen sprake. Een hoog niveau van beveiliging is hier vereist.

Hiermee heeft een ruwe classificatie van toepassingsgebieden plaatsgevonden. Er zal een fijnere classificatie-structuur van toepassingen moeten worden geformuleerd om vast te kunnen stellen wat het gewenste beveiligingsniveau van een bepaalde toepassing is en hiervoor zullen programma's van eisen moeten worden opgesteld. Het opstellen van een dergelijke classificatiestructuur en het vaststellen van programma's van eisen valt buiten het kader van dit onderzoek. Samenvattend kan worden gesteld dat er vooralsnog sprake is van drie onderscheiden toepassingsgebieden:

toepassing	**vorm**	**vereiste beveiligingsniveau**
'Look-alikes'	begeleid	laag
Kiosk in openbare ruimte	semi-begeleid	gemiddeld
PC in privé sfeer	niet begeleid	hoog

Voor al deze toepassingsgebieden geldt dat deze een zeer grote en zeer heterogene groep gebruikers omvatten. Dit brengt met zich mee dat in alle gevallen hoge eisen dienen te worden gesteld aan de biometrische techniek. In deze zin onderscheiden de toepassingsgebieden zich niet duidelijk.
Het is goed denkbaar dat verschillende toepassingen verschillende biometrische technieken vereisen. De veelheid van toepassingen waaraan wordt gedacht maakt het echter niet eenvoudig om tot scherp omlijnde keuzen te komen voor de verschillende toepassingsgebieden.

1.2 Doel van het onderzoek

De vraag dient beantwoord te worden welke biometrische techniek of technieken ingezet kunnen worden in de boven geschetste toepassingsgebieden:

- 'look-alikes'
- kiosk in openbare ruimte
- PC in privé sfeer

Het onderzoek dient argumenten aan te dragen op basis waarvan - voor de verschillende toepassingsgebieden - een keuze kan worden gemaakt voor geschikte biometrische technieken. Om deze vraag te kunnen beantwoorden dienen beoordelingscriteria te worden opgesteld, waarmee de verschillende beschikbare biometrische technieken kunnen worden beoordeeld op hun geschiktheid voor het toepassingsgebied.

1.3 Uitvoering van het onderzoek

Teneinde het onderzoek te structureren is een drietal onderzoeksfases gedefinieerd.

Fase 1 - Teneinde de benodigde beoordelingscriteria vast te stellen zijn allereerst de in dit kader belangrijkste parameters van biometrische technieken gedefinieerd en - waar mogelijk - gespecificeerd. Deze parameters zijn beveiliging, betrouwbaarheid, volgroeidheid van de technologie ('proven technology'), systeemarchitectuur, acceptatie door de gebruiker, eigenschappen van de apparatuur, en financiële aspecten. Deze parameters worden in hoofdstuk 2 besproken.

Fase 2 - In een reeks vraaggesprekken is nadere informatie vergaard bij deskundigen op verschillende toepassingsgebieden van biometrie m.b.t. biometrische technieken en de opgestelde beoordelingscriteria. In het bijzonder is hierbij ook aandacht geschonken aan het vergaren van informatie over grootschalige, reeds operationele biometrische toepassingen voor open, zeer heterogene gebruikersgroepen, in hoeverre en waarom deze toepassingen succesvol zijn en welke de eraan verbonden problemen zijn. Tevens is gevraagd welke de kritische succesfactoren zijn voor een grootschalige civiele toepassing van biometrie. In hoofdstuk 3 is een samenvatting van de resultaten van deze fase gegeven.

Fase 3 - In de derde en laatste fase van het onderzoek is een inventarisatie uitgevoerd van beschikbare biometrische technieken. Met behulp van de vastgestelde beoordelingscriteria is vervolgens nagegaan welke biometrische technieken eventueel in aanmerking komen voor de onderscheiden toepassingsgebieden. De resultaten van fase 3 zijn uitgewerkt in hoofdstuk 4.

2 Beoordelingscriteria

Teneinde een keuze te kunnen maken uit de veelheid van biometrische technieken, zijn beoordelingscriteria vastgesteld, waarmee een keuze voor de genoemde toepassingsgebieden kan worden onderbouwd. Deze maatlat is gebaseerd op de expertise van TNO alsmede op de informatie van verschillende experts op dit gebied, die door TNO zijn geïnterviewd.

2.1 Verificatie of identificatie

Allereerst dient de vraag te worden beantwoord of de gezochte toepassing van biometrie zal berusten op verificatie of identificatie.

Identificatie - Identificatie houdt het onderzoek in naar de ware identiteit van de een persoon op basis van een token (bijv. een document) of wachtwoord (bijv. een PIN-code). Identificatie houdt een één op veel controle in, waarbij de vraag wordt beantwoord: "Wie is de aanbieder?" De identificatieprocedure is in principe niet anoniem, daar een koppeling van biometrische gegevens aan persoonsgegevens bestaat, en de procedure geschiedt on-line.
Twee vormen van identificatie kunnen worden onderscheiden.

1. Identificatie aan de hand van de volledige opname van het biometrische kenmerk. Hierbij wordt de opname van het aangeboden biometrisch kenmerk vergeleken met in een database opgeslagen biometrische opnamen, die zijn gekoppeld aan persoonsgegevens. Een voorbeeld van een dergelijke vorm van identificatie is een "automated fingerprint identification system" (AFIS) zoals dat gebruikt wordt voor forensisch onderzoek. Deze vorm van identificatie komt, op juridische gronden, niet in aanmerking voor de toepassingen genoemd in beide toepassingsgebieden [2].
2. Identificatie aan de hand van een van het biometrische kenmerk afgeleide code, meestal aangeduid met biometrische sjabloon, of met de Engelse term *template*. Het kenmerkende verschil met de voorgaande vorm van identificatie is dat de oorspronkelijke biometrische gegevens niet uit de template kunnen worden afgeleid. Deze vorm van biometrische identificatie komt eventueel in aanmerking voor toepassingen genoemd in beide toepassingsgebieden.

Verificatie - Verificatie berust op de controle of de aanbieder van een token of wachtwoord ook de rechtmatige houder daarvan is. De controle is in principe een 1:1 controle, waarbij de vraag wordt beantwoord "Is de aanbieder degene die hij of zij op basis van het token/wachtwoord beweert te zijn?"
De verificatieprodecure berust altijd op de vergelijking van biometrische templates. Gecontroleerd wordt of de template van de aanbieder van het document overeenstemt met de op dat document opgeslagen template.

Verificatie kan - in principe - anoniem en off-line plaatsvinden. In veel gevallen is anonimiteit echter ongewenst, zoals bijvoorbeeld bij het aanvragen of verlengen van persoonspapieren of sociale bijstand. Het laat zich aanzien dat de toepassingen van biometrische controle door de overheid, in beide omschreven toepassingsgebieden, niet anoniem kunnen zijn. Anonimiteit is ook in tegenspraak met de koppeling van biometrie aan het gebruikte reisdocument dat immers essentiële persoonsgegevens bevat. Overigens kan de verificatieprocedure zo worden ingericht dat de op het document geplaatste persoonsgegevens eerst beschikbaar komen nadat de verificatieprocedure tot een positief resultaat heeft geleid. De houder geeft dan

met het aanbieden van het biometrische kenmerk aan dat deze vrijwillig de persoonsgegevens beschikbaar stelt [2].

Het al of niet noodzakelijk zijn van identificatie wordt voor een belangrijk deel bepaald door het antwoord op de vraag of er ergens vroeg in de keten van de uitgifte van het reisdocument reeds een deugdelijke identificatie heeft plaatsgevonden [2]. Indien dit laatste het geval is, kan daarna met verificatie worden volstaan. Vooralsnog wordt er van uitgegaan dat de reisdocumenten zijn uitgegeven op basis van een deugdelijke voorafgaande identificatie en dat de identificatie op afstand met het reisdocument op het proces van verificatie zal berusten. Opgemerkt wordt overigens dat twee van de geïnterviewde experts te kennen gaven dat dit proces in Nederland naar hun mening onvoldoende betrouwbaar is.

2.1.1 'look-alike' problematiek

Voor het toepassingsgebied 'look-alikes' is het antwoord op de vraag verificatie of identificatie op voorhand duidelijk. Hier dient de biometrische controle alleen de vraag te beantwoorden of de aanbieder van het document de rechtmatige houder is: biometrische verificatie.

De natuur herhaalt zich nooit: look-alikes verschillen altijd in details.

2.1.2 elektronische identificatie op afstand

Het antwoord op de vraag - verificatie of identificatie? - hang hier fundamenteel af van de vereiste toepassing.
In veel gevallen zal het voldoende zijn na te gaan of de aanbieder van de ID-kaart inderdaad de rechtmatige houder ervan is en kan met een biometrische verificatie worden volstaan.
Niet wordt hiermee voorkomen dat één enkele aanbieder meerdere - onder verschillende aliassen onrechtmatig verkregen - documenten in zijn bezit heeft. Dit laatste kan slechts worden opgespoord door een deugdelijke voorafgaande identificatie waarbij eventueel de aangeboden biometrische informatie wordt vergeleken met de in een database aanwezige biometrische informatie. Duplicaten (meervoudige identiteiten) worden daardoor (grotendeels) ontdekt.

Samenvattend kan worden gesteld dat biometrische technieken in beide toepassingsgebieden zullen berusten op een verificatieproces.

2.2 Niveau van beveiliging en foutpercentages

Biometrische technieken zijn vooralsnog behept met foutpercentages die op een veelheid van oorzaken berusten, zoals de zich steeds wijzigende vorm van aanbieden van het biometrisch kenmerk en kleine wijzigingen van dit kenmerk in de tijd. Deze foutpercentages bepalen voor een zeer belangrijk deel het goede functioneren van een biometrisch systeem. Daarom wordt in dit rapport ruim aandacht aan dit onderwerp besteed.

Na het vaststellen van het niveau van beveiliging in §1 voor de verschillende toepassingen, dient nader te worden ingevuld hoe dit vertaald dient te worden in de toelaatbare foutpercentages van de biometrische toepassing. Er kunnen verschillende foutpercentages onderscheiden worden:

1. Percentage ten onrechte toegelaten gebruikers, gewoonlijk aangeduid met *false accept rate* (FAR), neerkomend op succesvol bedrog (impostor penetration). Dit is een direct beveiligingsrisico. De FAR wordt berekend door een onderlinge vergelijking van de verschillen tussen alle gebruiker-templates. Uit de berekening volgt de gemiddelde kans dat een gebruiker zondermeer voor een ander kan doorgaan. De uitkomsten van deze berekening worden wel aangeduid met "zero-effort FAR" in contrast met de veel hogere FAR die het gevolg kan zijn van een vastberaden aanval.
2. Percentage ten onrechte geweigerde gebruikers, gewoonlijk aangeduid met *false reject rate* (FRR), neerkomend op ten onrechte afwijzing van een legitieme gebruiker (customer insult, operational failure). Dit is in eerste instantie een aspect van gebruikersvriendelijkheid van het systeem. Wanneer de FRR echter hoog is, wordt de 'fall-back' procedure zwaar belast, hetgeen eveneens een beveiligingsrisico kan inhouden.
3. *Equal error rate*, het foutpercentage dat optreedt wanneer de biometrische apparatuur zo wordt ingesteld dat FRR en FAR gelijk zijn. Deze parameter wordt vaak gebruikt om met één enkel getal de prestatie van biometrische apparatuur aan te duiden. Het belang van deze parameter is echter gering en deze zal in dit rapport niet worden gebruikt.
4. *Failure to enroll* (FTE), het percentage gebruikers dat in het geheel niet in het biometrische systeem ingevoerd kan worden, bijvoorbeeld door gebrek aan adequate biometrische kenmerken. Op vingerscan apparatuur bijvoorbeeld hebben ouderen, bouwvakkers en Aziaten vaker problemen met registratie. Te droge en te natte vingers kunnen ook een probleem vormen. Handgeometrie-apparatuur is voorts ongeschikt voor vrouwen met kleine handen, gezichtsherkenning vormt een probleem voor gesluierde vrouwen, enz. De FTE vormt ook een aspect van beveiliging, waar kwaadwillige gebruikers bewust trachten buiten het systeem te blijven.
   FTE specificaties van biometrische apparatuur zijn nauwelijks of niet beschikbaar. De FTE zal sterk afhangen van het gebruikersprofiel en lijkt niet verwaarloosbaar. In eerste instantie wordt de FTE pro memorie meegenomen als beoordelingscriterium. In het tijdschrift Biometric Technology Today (Btt) wordt een aantal malen de FTE van biometrische toepassingen genoemd:

Bron	**Biometrie**	**FTE**	**toepassing**
Btt vol. 7, nr. 5	Vingerscan	<1%	toegangscontrole in bank
Btt vol 6, nr. 10	silicon finger sensors	5-10%	toegangscontrole personeel
Btt vol 6, nr. 9	AFIS twee-vinger systeem	1.5%	sociale voorzieningen

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.

2.2.1 'fall-back' procedures

Daar biometrie niet foutloos functioneert, dient – ongeacht de biometrische toepassing – in adequate 'fall-back' procedures te zijn voorzien. De verdeling van bedriegers en afgewezen authentieke gebruikers over het totaal percentage afwijzingen is uiteraard onbekend. Bedriegers zullen alle moeite doen om als 'false reject' beschouwd te worden. 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. De hoogte van de FAR zal dan bepaald worden door de 'fall-back'

procedure en niet door de biometrische apparatuur. Grijpink [3] merkt over het belang van een adequate 'fall-back' procedure het volgende op:

> *"Als het verificatieproces niet vlekkeloos verloopt, blijkt men steevast terug te vallen op gebrekkige werkwijzen met een grote kans op fouten, zoals visuele herkenning aan de hand van een foto of het rechtstreeks ontlenen van gegevens aan een niet te controleren of een ongecontroleerd document. Insiders weten hoe gemakkelijk de menselijke geest ziet wat hij verwacht te zien en hoe moeilijk het is 'look-alikes' uit elkaar te houden."*

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

2.2.2 specificatie van foutpercentages

In het volgende worden specificaties gegeven voor de onderscheiden beveiligingsniveaus. Deze specificaties worden nader toegelicht, maar kunnen zeker niet worden beschouwd als "in steen gehouwen". De specificaties hebben een voorlopig karakter met als doel de gedachten te richten en moeten tenslotte nader worden bepaald op basis van een nauwkeurige beschouwing van het vereiste functioneren van iedere toepassing op zichzelf. Een dergelijke beschouwing vormt geen onderdeel van het voorliggende onderzoek.

'Look-alike' problematiek

Zoals in §1 reeds is betoogd, kan in dit toepassingsgebied naar verwachting worden volstaan met een betrekkelijk laag niveau van beveiliging, daar adequate 'fall-back' procedures mogelijk zijn. Er is sprake van een toepassing met een laag beveiligingsniveau wanneer de beveiliging van de toepassing niet alleen berust op de toegepaste technologie, maar tevens op de permanente aanwezigheid van begeleiding door een controleur (bijv. bij paspoortcontrole), of indien de waarde van de geboden dienst gering is. Het afbreukrisico van een toepassing die een laag beveiligingsniveau vereist, is gering. Indien de beveiliging van de toepassing faalt, is de imagoschade van de aanbieder van de toepassing gering.

De volgende vereisten hangen samen met een laag niveau van beveiliging waar voortdurend toezicht aanwezig is:

- FAR 1 : 1000
- FRR 1 : 20
- FTE p.m.
- geavanceerde biometrische apparatuur kan worden gebruikt

Toelichting - Het uitgangspunt is dat de biometrische verificatie onder permanent toezicht plaatsvindt en dat in uitstekende 'fall-back' procedures is voorzien. Voorts wordt ervan uitgegaan dat de controle op 'look-alikes' zal plaatsvinden op basis van selectie in geval van twijfel en niet op alle aanbieders van een reisdocument. Een FAR van 0,1% lijkt zeer acceptabel wanneer wordt bedacht dat, van de voorkomende twijfelgevallen die een nadere biometrische controle ondergaan, dan slechts één op de duizend ten onrechte door het biometrische systeem wordt geaccepteerd. Hierbij moet echter bedacht worden dat in het geval van 'look-alikes' de biometrische kenmerken niet altijd onafhankelijk zullen zijn, maar juist afhankelijk

vanwege een vaak voorkomende erfelijke relatie. Dit is niet slechts het geval met gelaatstrekken, maar bijvoorbeeld ook met de algemene structuur van vingerpatronen of met de vorm van de hand. In werkelijkheid kan de FAR daardoor ongunstiger uitvallen.
Een nader onderzoek brengt een zeker ongemak mee voor degene die (ten onrechte) dit onderzoek dient te ondergaan. Een FRR van 5% lijkt onder gecontroleerde omstandigheden geen bezwaar zijn, daar dit betekent dat slechts één op de 20 selectieve controles ten onrechte nader onderzoek met zich meebrengt.
Overigens dient nader te worden overwogen hoeveel ongemak dit onderzoek precies met zich meebrengt en hoeveel false rejects op basis van het gespecificeerde foutpercentage binnen een bepaalde periode per controlepunt redelijkerwijs mogen optreden.

Elektronische verificatie op afstand
In dit toepassingsgebied worden twee verschillende situaties onderscheiden: toepassingen in een kiosk in publieke ruimtes en toepassingen in de privé sfeer. In deze beide toepassingen vindt de biometrische controle plaats op alle aanbieders van een identiteitsdocument.
Een false reject in dit toepassingsgebied brengt ongemak met zich mee voor de documenthouder en veroorzaakt eveneens een zekere afbreukschade aan het systeem. Daar het hier om het verkrijgen van overheidsdiensten op afstand gaat, zal de ten onrechte afgewezen burger dit - naar verwachting - al snel als discriminerend en onacceptabel ervaren. De vraag dient te worden beantwoord hoe frequent - naar verwachting - het gebruik van het reisdocument voor verificatie op afstand zal zijn en hoeveel false rejects per tijdseenheid op een bepaald controlepunt nog acceptabel worden geacht.

<u>Biometrische apparatuur in openbare ruimte</u>
Zoals in §1 reeds is betoogd, dient in dit toepassingsgebied naar verwachting een gemiddeld niveau van beveiliging te worden gerealiseerd. Er is sprake van een toepassing met een gemiddeld niveau van beveiliging wanneer de beveiliging van de toepassing niet alleen berust op de toegepaste technologie, maar mede plaatsvindt in een semi-gecontroleerde omgeving (bijv. openbare ruimte in een gemeentehuis), of indien de waarde van de dienst gemiddeld is. Het afbreukrisico van een toepassing met gemiddelde beveiliging is matig. Indien de beveilig van de toepassing faalt, is de imago-schade voor de aanbieder van de toepassing beheersbaar.

De volgende vereisten hangen samen met een gemiddeld niveau van beveiliging bij toepassing in publieke ruimtes:

- FAR 1 : 10.000
- FRR 1 : 200
- FTE p.m.
- geavanceerde biometrische apparatuur kan worden gebruikt

Voorbeeld toepassing: een aanvraag van een geboorteakte op het gemeentehuis, een brondocument dat als uitgangspunt kan dienen voor het verkrijgen van een wettig algemeen identiteitsbewijs.

Toelichting - Het uitgangspunt is dat de biometrische verificatie onder semi-gecontroleerde omstandigheden plaatsvindt, waarbij een niet continu toezicht op afstand bestaat.

De geringere FAR van 0,01% lijkt in deze toepassing noodzakelijk omdat de biometrische controle niet wordt begeleid en niet slechts twijfelgevallen worden geverifieerd, maar zonder uitzondering alle gebruikers.
Tevens wordt aangenomen dat in redelijke 'fall-back' procedures aan een bemand loket is voorzien. Deze 'fall-back' procedures worden echter uitgevoerd door ambtenaren die daarnaast andere activiteiten verrichten. In deze niet begeleide toepassing brengt een nader onderzoek daarom niet alleen een zeker ongemak mee voor degene die ten onrechte dit onderzoek dient te ondergaan, maar belast tevens de ambtenaar die part time de 'fall-back' procedure uitvoert. Ook is het gevaar niet denkbeeldig dat, bij een relatief hoge FRR, het gebruik van de automatische kiosk snel zal dalen, en de burger zich zonder meer voor de 'fall-back' procedure zal gaan aanmelden. Een relatief geringe FRR van 0,5% lijkt daarom onder deze omstandigheden noodzakelijk. Het toegestane aantal niet-succesvolle verificatiepogingen dient beperkt te blijven (bijvoorbeeld tot drie). Bij overschrijden van dit aantal dient het document automatisch te worden uitgesloten van het verdere verkrijgen van diensten op afstand.

Privé biometrische apparatuur
Zoals in §1 reeds is betoogd, dient in dit toepassingsgebied naar verwachting een hoog niveau van beveiliging te worden gerealiseerd. Er is sprake van een toepassing met een hoog niveau van beveiliging wanneer de beveiliging van de toepassing volledig rust op de toegepaste technologie, of indien de waarde van de dienst hoog is. Het afbreukrisico is hier hoog. Indien de beveiliging van de toepassing faalt, is de imago-schade van de aanbieder van de toepassing groot.

De volgende vereisten hangen samen met een hoog niveau van beveiliging in een onbeheersbare privé omgeving:
- FAR 1 : 100.000
- FRR 1 : 2.000
- FTE p.m.
- goedkope, direct verkrijgbare biometrische apparatuur ('plug-and-play')

Voorbeeld toepassing: stemmen via het internet

Toelichting - De toepassing is volledig ongecontroleerd en daardoor zeer kwetsbaar voor pogingen tot identiteitsfraude. De nadelige gevolgen van een succesvolle frauduleuze handeling op basis van een valse identiteit kunnen groot zijn en tevens onacceptabele afbreukschade aan het systeem betekenen. De FAR dient hierom zeer laag te zijn, bijvoorbeeld 0,001%.
Opgemerkt wordt dat het realiseren van een lage FAR niet geheel op de biometrische techniek hoeft te berusten. De beveiliging tegen identiteitsfraude kan met een PKI (public key infrastructure) worden verhoogd, waarbij biometrie in combinatie met een token (bijv. smart card) en kennis (bijv. een pass phrase) wordt toegepast.
'Fall-back' procedures zijn binnen deze toepassing in feite niet beschikbaar, waardoor een zware wissel op het succes ervan wordt getrokken. Wanneer deze toepassing niet functioneert, dient de gebruiker terug te vallen op een andere toepassing waarmee de dienst kan worden verkregen (bijvoorbeeld het gemeentehuis of een stembureau). De FRR dient daarom zeer laag te zijn, daar de toepassing anders voor teveel gebruikers zinloos wordt. Zelfs een FRR van 0,05% is daarom voor deze toepassing mogelijk nog te hoog. De noodzaak tot het gebruik van relatief goedkope biometrische apparatuur in dit toepassingsgebied zal het echter niet eenvoudiger maken om zulke lage foutmarges te realiseren.

Het toegestane aantal niet-succesvolle pogingen tot verificatie dient beperkt te blijven. Bij overschrijden van dit aantal dient het document automatisch te worden uitgesloten van het verkrijgen van diensten op afstand.
Een overweging, specifiek voor dit toepassingsgebied, is dat de biometrische apparatuur naar verwachting door de documenthouder zelf is aangeschaft. Het niet of niet regelmatig functioneren ervan brengt dus niet slechts ongemak met zich mee, maar tevens financiële schade. Dit zal zeker onacceptabel worden geacht.

2.2.3 betrouwbaarheid van foutpercentages

De foutpercentages van biometrische apparatuur worden frequent gebruikt om de prestatie van biometrische apparatuur aan te duiden. Deze getallen zijn echter zeer onzeker en sterk afhankelijk van de wijze waarop ze gemeten zijn evenals van de gebruikersgroep [4,5]. Is de meting van de foutpercentages bijvoorbeeld gebaseerd op het doorzoeken van een bibliotheek van templates, of op een laboratoriumonderzoek door gebruikers die met de apparatuur vertrouwd zijn, of gebaseerd op een representatieve pilot met een grote en heterogene groep gebruikers? De laatste test levert zonder uitzondering aanzienlijk ongunstiger resultaten dan de eerdere.
Een netelige vraag is vervolgens, of the FRR en de FAR zijn gemeten met een gemeenschappelijke drempel-instelling van de apparatuur. Het is voorgekomen dat een lage FAR en FRR werden gespecificeerd, zonder dat daarbij werd vermeld dat deze uitkomsten waren verkregen met verschillende drempel-instellingen en dus niet gelijktijdig konden worden gerealiseerd [4,5].
De vele specificaties van foutpercentages die men in literatuur en brochures tegenkomt kunnen niet worden vergeleken of betrouwbaar worden geacht zonder nadere opgave van de wijze waarop ze zijn verkregen. Veelal zijn deze gegevens niet beschikbaar. Het hanteren van foutpercentages teneinde biometrische systemen te vergelijken is daarom een riskante zaak. Enerzijds is daar de apparatuur met haar eigen prestatie, een systeemgebonden FRR, anderzijds is daar de gebruiker, eveneens met zijn eigen (wan)prestatie.

Een reeks factoren bepaalt de invloed van de gebruiker in zijn omgeving op de prestatie van biometrische apparatuur, in het bijzonder de FRR.

1. De gebruiker is aanvankelijk minder vertrouwd met de apparatuur, waardoor de FRR hoger uitvalt dan verwacht en eerst geleidelijk daalt nadat de gebruikers vertrouwd raken met het systeem. Adequate begeleiding tijdens registratie en gedurende het eerste gebruik is van groot belang. In het INSPASS (Immigration and Naturalization Service Passenger Accelerated Service System) project bijvoorbeeld is onbegeleide vingerscanning niet mogelijk gebleken. Personen die de apparatuur niet regelmatig gebruikten bleken vaak problemen te hebben hun kenmerk op de juiste wijze aan te bieden [6].
   In het ideale geval is biometrische apparatuur zo ontworpen dat deze op ergonomische wijze tegemoet komt aan de eisen van de gebruiker die er voor de eerste maal mee te maken krijgt. Sommige gebruikers zullen echter altijd "onhandig" blijven omgaan met de apparatuur, zeker wanneer deze niet frequent wordt gebruikt.
2. Sommige biometrische technieken zullen door bepaalde groepen mensen niet of nauwelijks gebruikt kunnen worden (bijvoorbeeld personen met een weinig geprofileerd vingerpatroon). Dit kan tot een niet onbelangrijk percentage FTE leiden.
3. Bij sommige biometrische technieken, zoals hand- en vingergeometrie en gezichtsherkenning, spelen verandering in de tijd en veroudering een rol. Wanneer de gebruiker enige tijd met een zware koffer heeft gesjouwd is de handgeometrie tijdelijk veranderd. Maar ook verandert de handgeometrie met de

tijd, wanneer de vingernagels langer groeien, en met de leeftijd. Het gelaat kan, door verwonding, aan vrij plotselinge verandering onderhevig zijn, maar ook de fysieke constitutie en veroudering kunnen het gelaat op den duur ingrijpend veranderen. Dergelijke veranderingen kunnen in zekere mate worden opgevangen door, iedere keer dat de gebruiker verschijnt, een update te maken van de historische template aan de hand van de actuele template. Deze update-strategie kan in principe voor iedere biometrische techniek worden gerealiseerd. Voor een irispatroon is dit uiteraard niet zinvol daar dit patroon zeer robuust is, terwijl het maken van een regelmatige update bijvoorbeeld voor de handgeometrie meestal wèl wordt gedaan. Wanneer echter de gebruiker niet frequent genoeg van het systeem gebruik maakt, helpt deze aanpak niet en volgt toch een afwijzing ten onrechte.
Juist bij de in dit rapport beschouwde toepassingsgebieden moet men zich afvragen of de frequentie van het gebruik niet zodanig gering zal zijn dat dit voor sommige vormen van biometrie een probleem gaat vormen.

4. De foutpercentages kunnen sterk afhangen van het al of niet aanwezig zijn van een begeleider bij het systeem. Deze kan de onhandige gebruiker aanwijzingen geven en voorts tegenwerking en bedrog signaleren.
5. Onderscheid dient te worden gemaakt tussen de groep gebruikers die er baat bij heeft mee te werken aan het systeem en de groep die geneigd is tot tegenwerking of zelfs bedrog. Tegenwerking kan bijvoorbeeld ontstaan door een min of meer onbewuste weerstand op grond van hygiënische of psychologische overwegingen. Bedrog, teneinde een opzettelijk reject te veroorzaken, kan voortvloeien uit de wens gebruik te maken van de 'fall-back' procedure omdat deze naar verwachting een geringere beveiliging heeft.

Hoezeer de prestatie van biometrische systemen van psychologische elementen afhankelijk is wordt aangevoerd door Ashbourn, die op basis van veel praktijkervaring een *user psychology index* (UPI index) introduceert, een hulpmiddel waarmee een ruwe schatting kan worden gemaakt van de FRR die in een toepassing verwacht kan worden als functie van een aantal cruciale gebruikers- en omgevingselementen [7]. Ashbourn onderscheidt, in twaalf gebruikersprofielen, vier psychologische elementen, namelijk de psychologische status van de gebruiker, die kan variëren tussen welwillend en vijandig, de bekendheid van de gebruiker met de apparatuur en zijn werking, de invloed van de omgeving op de gebruiker en de betekenis van het resultaat van de verificatie voor de gebruiker. Verschillende combinaties van deze gebruikselementen leiden tot een op ervaring gebaseerde UPI index, een factor waarmee de apparaat-gebonden FRR dient te worden vermenigvuldigd teneinde een schatting te krijgen van de in de praktijk te verwachten FRR. Tabel I geeft een overzicht van de UPI index als functie van deze vier gebruikerselementen.

De eerste rij in deze tabel geeft de situatie weer van een laboratoriumonderzoek waarbij de systeemgebonden foutpercentages zo nauwkeurig mogelijk worden bepaald door welingelichte gebruikers die goed met het systeem bekend en vertrouwd zijn en dit in een gemakkelijke omgeving kunnen testen, zonder dat de resultaten voor de gebruiker persoonlijk kritisch zijn (UPI index = 1). Veelal betreft het hier de specificaties die door de fabrikant van de biometrische apparatuur worden gegeven.

Tabel 1 - *User Psychology index volgens Ashbourn*

profiel	status van de gebruiker	Bekendheid	omgeving	resultaat	UPI index
1	welingelicht/welwillend	Groot	ontspannen/gemakkelijk	niet kritisch	1
2	welingelicht/welwillend	Normaal	ontspannen/gemakkelijk	kritisch	1,25

3	welingelicht/welwillend	Gering	ontspannen/gemakkelijk	niet kritisch	1,5
4	welingelicht/welwillend	Gering	ontspannen/gemakkelijk	kritisch	2
5	ongeïnteresseerd	Gering	ontspannen/gemakkelijk	niet kritisch	2,25
6	ongeïnteresseerd	Gering	ontspannen/gemakkelijk	kritisch	2,5
7	ongeïnteresseerd	Gering	ongemakkelijk	niet kritisch	3
8	ongeïnteresseerd	Gering	ongemakkelijk	kritisch	3,5
9	ongeïnteresseerd	Gering	ongemakkelijk, additionele externe druk	kritisch	5
10	vijandig	Gering	ongemakkelijk	kritisch	7
11	vijandig	Gering	ongemakkelijk	niet kritisch	10
12	vijandig	Gering	ongemakkelijk, additionele externe druk	niet kritisch	15

In de in dit rapport besproken toepassingsgebieden is de gemiddelde gebruiker naar verwachting ongeïnteresseerd, heeft een geringe kennis van de apparatuur en zijn werking, terwijl het resultaat van de verificatie kritisch is. In tabel 2 is een overzicht gegeven van de vermoedelijke profielen van gebruikersgroepen in de verschillende hier besproken toepassingen.

Tabel 2 – gebruikersprofielen		
toepassingsgebied	**profiel**	**UPI index**
'look-alikes'	8, 9 en 10	3,5 – 7
Publieke ruimtes	8 en 9	3,5 – 5
Privé	2, 4 en 6	1,25 - 2,5

In dit psychologische profiel is geen rekening gehouden met de mate van begeleiding tijdens invoer van de gebruiker op het systeem en in de beginfase van het gebruik, evenmin als met de regelmaat van het gebruik. Er zijn goede redenen om aan te nemen dat bij slechte begeleiding en weinig frequent gebruik de UPI index verder toeneemt. Het ziet er daarom naar uit dat de prestatie van biometrische systemen in de praktijk niet zozeer wordt bepaald door de apparatuur zelf, maar grotendeels door de gebruiker en de praktijkomstandigheden. Tengevolge daarvan lijken de false reject cijfers van verschillende biometrische systemen elkaar in de harde praktijk niet bijzonder te ontlopen en zich in een gebied van ruwweg 1% tot 5% te bevinden (zie ook appendix III). Het spreekt voorts vanzelf dat ook de FTE sterk wordt beïnvloed door het gebruikersprofiel.
Het is in dit verband illustratief een blik te werpen op een recente test op de toepassing van biometrie bij dagelijkse grenscontrole op Palestijnse arbeiders in Israël, waarbij 11 leveranciers betrokken waren met 13 producten die 6 verschillende biometrische technieken omvatten: vingerafdruk, gezichtsherkenning, irisherkenning, palm geometrie, twee-vingergeometrie en stemherkenning) [8]. De gestelde betrouwbaarheidseisen van deze test zijn weergegeven in tabel 3. Geen enkele getest product bleek in staat de nagestreefde betrouwbaarheid te halen, terwijl slechts 2 producten aan de minimale betrouwbaarheidseisen voldeden (gezichtsherkenning en handgeometrie). Het psychologisch gebruikersprofiel van de gebruikersgroep bij deze test is waarschijnlijk 8-10 geweest, corresponderend met een UPI van 3,5 tot 7.

Tabel 3 - Testcriteria biometrie grenscontrole in Israël [8]		
	minimale betrouwbaarheidseisen	nagestreefde betrouwbaarheid
FRR*)	< 3%	< 0,1%

FAR	< 1%	< 0,1%

*) inclusief FTE.

Uit het voorgaande blijkt dat de FRR als betrouwbaar beoordelingscriterium voor biometrische technieken in feite niet beschikbaar is. Ook over de FAR van biometrische technieken is te weinig bekend om deze als objectief en betrouwbaar beoordelingscriterium te accepteren voor het onderling vergelijken van biometrische technieken.

De beste aanpak om nadere gegevens te verkrijgen is het vragen van referenties bij leveranciers en het nagaan bij de genoemde gebruikers van het biometrische systeem wat hun ervaringen zijn. Dit vooronderstelt reeds de noodzaak van volgroeide technologie ('proven technology'). Nog maar weinig biometrische technieken hebben echter rigoureuze, onafhankelijke tests ondergaan, waarbij de duurzaamheid, uniciteit, toegankelijkheid en beschikbaarheid van het biometrische kenmerk, en foutpercentages en accepteerbaarheid van de biometrische technologie zijn getest [9] (zie ook §2.4).
Tenslotte staat de weg open één of meer biometrische systemen in een pilot nader te onderzoeken. Het samenstellen van een representatief gebruikersprofiel is daarbij, zoals aangetoond, van zeer groot belang, maar dit is niet eenvoudig. Een in de tijd stabiele testpopulatie is moeilijk samen te stellen en het begrip van de factoren die de prestatie van biometrische systemen beïnvloeden is nog zo gebrekkig, dat een goede schatting altijd een groot probleem zal blijven, zodat de voorspellende waarde van biometrische pilots beperkt zal blijven [9].

2.3 Risico van vandalisme en sabotage

Hoewel de weerstand van de biometrische apparatuur tegen misbruik zoals vandalisme en sabotage van belang is, kan hierover niets in kwantitatieve zin worden gezegd. Veel hangt af van het gebruikersprofiel en de gebruikersomgeving. In het algemeen geldt het volgende. Robuustheid is belangrijk wanneer het publiek direct contact heeft met de apparatuur (bijv. een handscanner of een vingerscan). De aanwezigheid van kwetsbare onderdelen (bijv. glasoppervlakken) die worden aangeraakt tijdens aanmelden maken het systeem minder robuust. Biometrische apparatuur die geen direct fysiek contact behoeft tijdens het aanmelden (bijv. een camera voor gezichtsherkenning) kan in het algemeen beschouwd worden als meer robuust dan apparatuur die fysiek contact vereist.

Naast het risico van misbruik van de biometrische apparatuur, bestaat het risico van misbruik van het reisdocument zelf. Het is voorspelbaar dat kwaadwillige gebruikers de biometrische functionaliteit van het reisdocument, zonder zichtbare sporen, onklaar zullen trachten te maken teneinde de biometrische controle te kunnen omzeilen. De gebruiker komt dan in een 'fall-back' procedure terecht die niet langer gebruik kan maken van biometrie en die daardoor mogelijk wezenlijk minder betrouwbaar wordt. Indien dit risico niet door een adequate procedure kan worden opgevangen is het denkbaar dat het functioneren van biometrie als maatregel tegen 'look-alikes' geheel wordt tenietgedaan. Op de keuze van de biometrische techniek heeft dit risico uiteraard geen invloed.

Kwaadwillige gebruikers die van de 'fall-back' procedure gebruik wensen te maken waarvan zij verwachten dat deze minder hoog beveiligd is, zullen eventueel ook trachten het biometrische kenmerk

zodanig aan te bieden dat een reject volgt. Het verdient hierom sterke aanbeveling een biometrische techniek toe te passen die geen actief handelen van de gebruiker vergt.

2.3.1 'look-alike' problematiek

Wanneer de biometrische apparatuur onder toezicht wordt gebruikt is de kans op misbruik van de apparatuur door vandalisme of sabotage naar verwachting gering of zelfs verwaarloosbaar.

2.3.2 elektronische verificatie op afstand

Hierbij doen zich wederom twee onderscheiden situaties voor: biometrische apparatuur in een publieke kiosk, semi-gecontroleerd en in de privé sfeer, geheel ongecontroleerd.

1. Biometrische apparatuur in publieke ruimtes

Wanneer de biometrische apparatuur voor het publiek algemeen toegankelijk is en niet permanent bewaakt, speelt de weerstand tegen misbruik als vandalisme een zekere rol. De kans op sabotage is in deze situatie gering daar het ongemerkt 'sleutelen' aan de apparatuur in een semi-gecontroleerde, publieke ruimte - naar verwachting - niet gemakkelijk of zelfs onmogelijk zal zijn.

2. Privé biometrische apparatuur

Voor biometrische apparatuur verbonden met bijvoorbeeld een PC in de privé sfeer bestaat het risico van vandalisme uiteraard niet, de apparatuur is immers eigendom van de gebruiker zelf. In deze situatie is het risico van sabotage echter hoog, daar de eigenaar ongelimiteerd en ongemerkt aan de apparatuur kan sleutelen. Wanneer deze toepassing dient te worden gerealiseerd, dient te worden nagegaan welke aanvallen worden verwacht en òf en hóe daartegen kan worden beveiligd.

Samenvattend kan het volgende worden gesteld.
Sommige biometrische technieken zullen minder bestand zijn tegen misbruik dan ander, in het bijzonder apparatuur die contact met de gebruiker vereist is hiervoor naar verwachting gevoelig. In de verschillende toepassingsgebieden is de kans op sabotage en vandalisme verschillend. In tabel 4 worden de verwachte kansen hierop samengevat.

Tabel 4 – Kans op misbruik apparatuur door de gebruiker		
Toepassingsgebied	**Vandalisme**	**Sabotage**
'look-alikes'	zeer gering	Afwezig
publieke kiosk	van betekenis	Gering
Prive PC	n.v.t.	Zeer hoog

2.4 Eigenschappen van het biometrische kenmerk

De eigenschappen van het biometrische kenmerk die in ogenschouw dienen te worden genomen zijn de gevoeligheid ervan voor identiteitsfraude en de uniciteit en de duurzaamheid ervan. Hiernaast kunnen beschikbaarheid, toegankelijkheid en acceptatie van het biometrische kenmerk een rol spelen. De meeste van deze eigenschappen hebben een meer algemene betekenis en kunnen niet direct worden verbonden met een van de specifieke toepassingsgebieden.

Gevoeligheid voor fraude - Voorkomen dient te worden dat identiteitsfraude kan worden gebaseerd op het gebruik van kopieën van het biometrische kenmerk (foto van gelaat of iris), op roof (vingers afhakken, etc), of op het steels verkrijgen daarvan (vingerafdrukken kopiëren, stem op band opnemen).
De kans op deze vorm van fraude is gering wanneer de biometrische apparatuur onder direct toezicht staat en is dus voor het toepassingsgebied 'look-alikes' niet van belang.
Bij elektronische verificatie op afstand is de kans op een dergelijke identiteitsfraude niet uitgesloten. Voorwaarde is derhalve dat de toegepaste biometrische techniek voorziet in een effectieve detectie van het levend zijn van het aangeboden biometrische kenmerk.

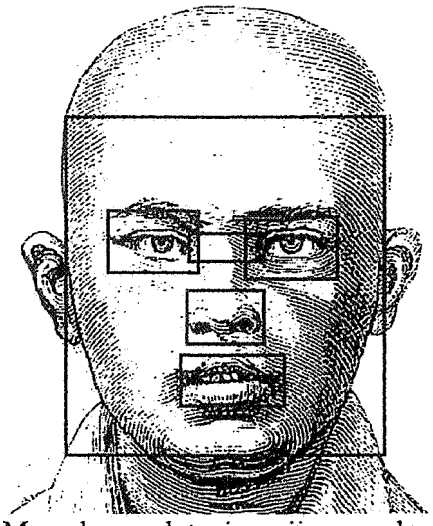
Uniciteit van het biometrisch kenmerk - Veelal wordt gesteld dat het biometrische kenmerk uniek dient te zijn. Dit is echter geen onafhankelijke parameter, daar de uniciteit van het kenmerk zich weerspiegelt in de foutpercentages, in het bijzonder in de FAR. Dit foutpercentage wordt echter ook door andere factoren bepaald, zoals technische factoren en gebruiksfactoren.

Biometrische kenmerken als geslacht, lichaamslengte en de kleur van de ogen, zoals deze wel in paspoorten worden vermeld, zijn nu niet bepaald uniek. Wat maakt een biometrisch kenmerk nu wèl uniek? Van essentieel belang voor het uniek zijn van biometrische kenmerken is het aantal typica dat kan worden beschreven en gemeten. Typica in een patroon van vingerlijnen zijn bijvoorbeeld vertakkingen, eindpunten en eilanden. Een vinger bevat enkele tientallen typica en een overeenkomst in de positie van meer dan 12 typica is reeds voldoende om een identiteit met volkomen zekerheid vast te stellen. Het aantal typica in het vlekkenpatroon van de iris bedraagt enige honderden, en aangenomen wordt daarom wel dat de iris van de mens nog unieker is dan zijn vinger.

Een eeneiige tweeling: de typica van de beide rechterwijsvingers verschillen significant.

Het vlekkenpatroon in de iris van het oog is mogelijk nog unieker dan het vingerlijnen-patroon.

Maar hoeveel typica zijn te beschrijven en te meten van het menselijk gelaat of van de geometrie van de hand? Vooralsnog zijn dit er minder, en de geometrische relatie van deze typica is niet willekeurig. Daarom zijn kenmerken als handgeometrie en gelaat in principe minder uniek. Een exact bewijs voor het uniek zijn van een kenmerk is nooit te leveren, de biometrische praktijk moet in de loop van de tijd de overtuiging bieden. Uniciteit van het biometrische kenmerk is een parameter die mee kan wegen wanneer een bijzonder lage FAR vereist is.



Maar hoeveel typica zijn nauwkeurig te beschrijven en te meten in het menselijk gelaat of in de geometrie van de hand?

Duurzaamheid en constantheid van het biometrisch kenmerk - Voor een goede werking van het biometrische systeem dient een biometrisch kenmerk robuust te zijn, d.w.z. in de tijd voldoende constant te blijven of er dient een regelmatige update van de template te kunnen plaats vinden. Fysieke kenmerken neigen tot grotere stabiliteit dan gedragskenmerken, hetgeen niet wil zeggen dat ze niet aan verandering onderhevig kunnen zijn. De geometrie van de hand is bijvoorbeeld afhankelijk van temperatuur, doorbloeding en ouderdom. Onze vingerpatronen bevinden zich op een kwetsbare plaats aan het eind van onze ledematen en kunnen daarom makkelijk worden beschadigd. De irispatronen in het oog daarentegen zijn zeer robuust en de mens getroost zich, onwillekeurig zowel als willekeurig, veel inspanning de ogen tegen schade te beschermen. Gedragskenmerken, hoewel deze een fysiologische basis hebben, neigen tot veranderen met de psychologische toestand van de gebruiker. Iemand die haast heeft of boos is zal bijvoorbeeld een andere dynamiek van handtekenen hebben of een andere stemkarakteristiek, dan iemand die kalm is.
Deze parameter, die ook wel wordt aangeduid met atrofie of veroudering van de template, is geen onafhankelijke parameter daar deze wordt weerspiegeld in het lange termijn foutpercentage, in het bijzonder in de FRR. Wanneer de gebruiker niet frequent van het systeem gebruik maakt, biedt updating van de template geen uitkomst. Duurzaamheid van het biometrische kenmerk weegt daarom mee voor zover een lage FRR vereist is en de gebruikerspopulatie een geringe gebruiksfrequentie heeft.

Beschikbaarheid van het biometrische kenmerk - Met de beschikbaarheid van het biometrisch kenmerk wordt gedoeld op het aantal onafhankelijke alternatieven dat beschikbaar is, wanneer het gebruikelijke kenmerk (tijdelijk) niet (volledig) beschikbaar is. Een persoon kan, bijvoorbeeld, tenminste zes onafhankelijke vingerafdrukken presenteren [9], twee onafhankelijke irispatronen, maar slechts één

geometrie van de hand (de andere hand is een min of meer getrouw spiegelbeeld daarvan) en slechts één gelaat.
Toegankelijkheid van het biometrische kenmerk - De eenvoud en het gemak waarmee een biometrisch kenmerk op de juiste wijze kan worden aangeboden aan de apparatuur wordt wel aangeduid met de toegankelijkheid ervan. De hand kan bijvoorbeeld zonder veel training correct worden aangeboden, maar veel mensen blijken aanvankelijk te menen dat de positie van het vingerpatroon op de vingertip zit [9]. Het aanbieden van het aderpatroon in het netvlies door het oog nabij de optiek van de apparatuur te brengen en op de juiste wijze scherp te stellen is zonder meer lastig. De toegankelijkheid wordt verbeterd door de apparatuur ergonomisch in te richten en door de gebruiker een adequate terugkoppeling te geven van de wijze waarop hij zijn biometrische kenmerk aanbiedt. Het verdient daarbij de voorkeur dat de apparatuur zo is ingericht dat deze zonder nadere instructie kan worden gebruikt. De noodzaak van een min of meer uitgebreide instructie heeft een ongunstige werking op het correcte gebruik, zeker wanneer dit niet zeer frequent is. Wanneer met deze factoren goed is rekening gehouden heeft dit een gunstige invloed op de FRR zowel als de FTE.

Acceptatie van het gebruik van een biometrisch kenmerk - Biometrische kenmerken verschillen m.b.t. de bereidheid van de gebruiker het bewuste biometrische kenmerk voor verificatie beschikbaar te stellen. Van vingerafdrukken wordt wel gezegd dat deze door de gebruiker vanouds worden geassocieerd met criminaliteit en dat hieruit een weerstand tegen het gebruik zou voortvloeien. Het gebruik van het irispatroon wordt door sommigen geassocieerd met iriscopie, een vorm van medische diagnostiek, waarbij - naar wordt beweerd - ziektes kunnen worden geconstateerd. Sommige gebruikers zullen daarom niet bereid zijn hun iris aan een onderzoek te onderwerpen. Bij sommige gebruikers zal de bereidheid gering zijn hun biometrisch kenmerk in contact te brengen met de biometrische apparatuur, bijvoorbeeld op grond van hygiënische overwegingen, of aan te bieden op grond van overwegingen van fysieke integriteit (bijv. vrees voor schade aan het oog door straling). De maatschappelijke acceptatie van biometrie is sterk afhankelijk van voorlichting en het verbonden zijn van persoonlijke voordelen aan de toepassing en lijkt in de loop van de tijd toe te nemen.

2.5 Betrouwbaarheid en 'proven technology'

De betrouwbaarheid van biometrische apparatuur wordt enerzijds bepaald door het discriminerend vermogen ervan en anderzijds door het storingsvrij functioneren.

Beveiligingsaspecten - De betrouwbaarheid vanuit het oogpunt van beveiliging, is de geschiktheid van het systeem om op lange termijn correct ongeautoriseerde gebruikers af te wijzen, dit wordt weerspiegeld in een lage FAR. Een systeem dat zo is afgesteld dat het iedere gebruiker afwijst is betrouwbaar (en hoog beveiligd) omdat het consequent alle bedriegers weert; een dergelijk systeem heeft echter geen discriminerend vermogen.
De geschiktheid geautoriseerde gebruikers te accepteren, weerspiegeld in een lage FRR, is geen direct middel tot beveiliging.

Aspecten van gebruikersacceptatie - Betrouwbaarheid vanuit het standpunt van gebruikersacceptatie is de geschiktheid van het systeem om op lange termijn correct de geautoriseerde gebruikers toe te laten. Dit wordt weerspiegeld in een lage FRR. Een systeem dat iedere gebruiker accepteert is betrouwbaar (en

gebruikersvriendelijk) omdat het consequent alle geautoriseerde gebruikers accepteert; een dergelijk systeem heeft echter geen discriminerend vermogen.
De geschiktheid van het systeem bedriegers te weren, weerspiegeld in een lage FAR, is geen middel tot gebruikersacceptatie.

Betrouwbaarheid zowel vanuit het standpunt van beveiliging als gebruikersacceptatie is daarom equivalent aan discriminerend vermogen op lange termijn. Dit discriminerend vermogen wordt gegeven door de systeemgebonden foutpercentages van het biometrisch systeem (FAR en FRR) zowel als door de constantheid van deze foutpercentages in de tijd. De betrouwbaarheid kan daarom, naast de foutpercentages, worden uitgedrukt in variabiliteit (de spreiding rond het gemiddelde) van de systeemgebonden foutpercentages in de tijd. Spreidingscijfers van de foutpercentages van biometrische apparatuur zijn nauwelijks of niet bekend en deze zullen in de huidige studie niet worden meegenomen. Aanbevolen wordt hier in de toekomst aandacht aan te besteden.

Failure to enroll - De FTE vormt in zekere zin ook een aspect van betrouwbaarheid. Een biometrische techniek die een hoge FTE met zich meebrengt, kan als minder betrouwbaar worden beschouwd.

De betrouwbaarheid van de biometrische apparatuur wordt niet alleen bepaald door de systeemgebonden foutpercentages en de spreiding daarvan in de tijd. De ongestoorde beschikbaarheid van het systeem in het gebruik speelt eveneens een rol. Het is niet de bedoeling dat de goede werking van een biometrisch systeem slechts kan worden gehandhaafd door voortdurend afregelen en onderhoud (schoonmaken) [5].
De weerstand van het systeem voor storingen wordt uitgedrukt in de parameters

- MTBF ('mean time between failure'), en
- MTTR ('mean time to repair').

De specificaties voor deze parameters zijn belangrijk, maar zullen zeer sterk afhangen van de uiteindelijke uitvoering van de biometrische systemen. Het mag niet worden verwacht dat deze parameters bekend zijn en deze zullen in de huidige studie niet worden meegenomen. Wel zullen deze parameters naar verwachting niet beduidend verschillen van die van de gebruikelijke IT apparatuur.

Nog een ander aspect van betrouwbaarheid is de mate van inspanning die nodig is om het biometrisch systeem te omzeilen met een imitatie van de biometrische karakteristiek. Wanneer echter de vereiste, afdoende detectie op "leven en welzijn" aanwezig is, zal de kans op succes met imitaties zeer gering zijn.

Uit het voorgaande volgt, dat voor de besproken toepassingsgebieden alleen systemen in aanmerking komen waarvoor gegevens over de betrouwbaarheid beschikbaar zijn uit de praktijk. Met andere woorden, alleen volgroeide technologie ('proven technology') komt in aanmerking. Wanneer geen kwantitatieve gegevens kunnen worden verkregen m.b.t. de spreiding van de foutpercentages in de tijd, kunnen de volgende kenmerken in de beoordeling worden betrokken:

- Aantal producenten - Er dient een duidelijke concurrentie te bestaan; biometrische technieken waarvoor slechts één of twee producenten bestaan, komen niet in aanmerking.

- Onmiddellijke commerciële beschikbaarheid.
- Aantal operationele biometrische toepassingen die worden gekenmerkt door een voldoend grote schaal.
- Eventuele testrapporten.

2.6 Systeemarchitectuur

'Stand-alone' vs netwerk - De gewenste architectuur van het systeem wordt in de eerste plaats bepaald door de gebruiksomgeving. Biometrische apparatuur bij (mobiele) grenscontrole zal mogelijk 'stand-alone' kunnen zijn, terwijl toepassingen in de sfeer van verificatie identiteit bij het verkrijgen van overheidsdiensten (aanvraag paspoort, verkrijgen uitkering) mogelijk de toepassing van netwerken zullen vereisen, waarbij tevens dient te worden bezien of deze netwerken centraal, gedistribueerd of hybride zullen zijn [10]. Een dergelijke keuze is onafhankelijk van het toegepaste biometrische kenmerk en deze keuze zal daarom geen beoordelingscriterium zijn. Wel dient voor sommige toepassingsgebieden te worden geëist dat de biometrische apparatuur geschikt is voor aansluiting op een netwerk.

Opslag van gegevens - De systeemarchitectuur wordt mede bepaald door de wijze van opslag van de gegevens. Voor de onderzochte toepassingsgebieden geldt dat de biometrische template wordt opgeslagen in het gebruikte token (paspoort, ID-Kaart). De biometrische controle zal dus off-line gebeuren. Deze opslag kan plaatsvinden in een chip, een magneetstrip, een optisch geheugen, of in een (tweedimensionale) barcode. De keuze voor de wijze van opslag van gegevens is afhankelijk van de grootte van de template en daarmee van de biometrische techniek. Een voorkeur voor een bepaalde wijze van opslag voor de beide toepassingsgebieden bestaat momenteel niet bij BZK; de wijze van opslag is daarom geen beoordelingscriterium, maar volgt (deels) uit de gemaakte keuze(n) voor een biometrisch systeem.

Hoe de noodzakelijke biometrische systemen operationeel kunnen worden opgezet, welke architectuur daarvoor is vereist en hoe het beheer en de infrastructuur daarvan geregeld dienen te worden hangt in hoge mate af van het gebied van toepassing, de te leveren diensten en de aan de levering te stellen eisen. In het geval van 'look-alikes' bij grensverkeer is het voldoende te verifiëren of de houder van het reisdocument de rechtmatige houder is. In sommige gevallen zal door de provider van een overheidsdienst echter niet slechts worden gevraagd of de houder van het document de rechtmatige houder is (verificatie), maar onafhankelijk daarvan kan ook de vraag of de houder recht heeft op de gevraagde dienst een rol spelen, zodat (pseudo)identificatie mede noodzakelijk wordt (bijv. bij uitkeringen). Door het biometrisch kenmerk aan te bieden geeft de gebruiker de provider toestemming de noodzakelijke persoonsinformatie te raadplegen. Deze laatste actie veronderstelt enige vorm van centrale opslag van persoonsinformatie. Tabel 5 geeft een overzicht van de verschillende mogelijkheden.
De toegepaste biometrische techniek speelt bij deze keuzen geen rol.

Tabel 5 – Systeemarchitectuur

toepassingsgebied	**Architectuur**	**beheer**
'look-alikes', grensverkeer	'stand-alone'	centraal, door provider
'look-alikes', dienstverlening	'stand-alone'/centraal	centraal, door provider
publieke kiosk	'stand-alone'/centraal	centraal, door provider
Prive PC	'stand-alone'/centraal	geen

2.7 Maatschappelijke acceptatie

De acceptatie van een biometrisch systeem door de gebruiker is sterk afhankelijk van de toegepaste biometrische techniek, de toepassing en de gebruiker [7,10].

De techniek

- De biometrische techniek (niet opdringerig, hygiënisch, etc.)
- Het gebruiksgemak (ergonomie, transactiesnelheid, betrouwbaarheid, etc.)
- Perceptie van veiligheid en beveiliging (hygiëne, detectie op "leven en welzijn", minder kans op fraude, etc.)

De toepassing

- De aantrekkelijkheid van het systeem (eventuele bijzondere voordelen)
- Het nut voor de gebruiker (lage FTE, zodat weinig individuen of groepen van gebruik zijn uitgesloten)
- Juridische aspecten (fysieke integriteit, privacy, anonimiteit, niet-discriminerend).

De gebruiker

- Het gebruikersprofiel.
  Met betrekking tot de samenhang van het gebruikersprofiel en maatschappelijke acceptatie kan worden verwacht dat de acceptatie afneemt met hoger profielnummer (zie tabel 1), waarbij de psychologische status van de gebruiker van welwillend tot vijandig varieert. Indien dit juist is zullen, volgens tabel 2, de toepassingsgebieden 'look-alikes' en publieke ruimten (UPI index 3,5 - 7) vermoedelijk met een geringere maatschappelijke acceptatie gepaard gaan dan het toepassingsgebied privé PC (UPI-index 2-2,5).
  Met betrekking tot de 'look-alike' problematiek speelt overigens maatschappelijke acceptatie mogelijk een minder belangrijke rol. Het is denkbaar dat de burger of reiziger, die dit onderzoek ondergaat, ertoe neigt dit als een noodzakelijk kwaad beschouwen. Slechts perceptie van veiligheid en beveiliging lijkt in dit toepassingsgebied van enig belang. Met betrekking tot elektronische verificatie op afstand lijkt het wel zeker dat alle genoemde parameters, die tot maatschappelijke acceptatie leiden, van belang zijn.
- De schuldvraag bij optredende fouten.
  Naast de bovengenoemde psychologische factoren speelt nog de volgende. Gebruikers blijken zichzelf de schuld te geven van vergissingen met de PIN-code, ze neigen bij fouten van een token, het token de schuld daarvan te geven, en bij fouten voortkomend uit het gebruik van biometrie, geven zij het systeem de schuld. Biometrische technieken zijn daarom het meest gevoelig voor afbreukschade t.g.v. reject rates.

Sommige van deze parameters kunnen worden gekwantificeerd door het instellen van een representatief publieksonderzoek. Dergelijke onderzoeken zijn wel gedaan, maar de uitkomsten ervan hangen mede af van het toepassingsgebied, culturele achtergronden en het gebruikersprofiel. Hoe moeilijk het is een representatieve testgroep te formeren is reeds vermeld [9]. Tevens mag in de tijd een toename worden verwacht in acceptatie van biometrische technieken naarmate deze bekender worden; men aan de gedachte gaat wennen mede dank zij goede voorlichting en doordat het nut van de toepassing wordt ingezien en deze tevens gemak gaat opleveren. Een onderzoek van enige jaren terug kan daardoor nu achterhaald zijn of niet van toepassing omdat het een niet representatieve populatie betreft.
Als kwalitatieve maatstaf kunnen de bovengenoemde parameters worden toegepast bij de vergelijking van verschillende biometrische systemen. Ieder van de parameters van techniek en toepassing is een middel tot het doel: acceptatie door de gebruiker.

Met betrekking tot de juridische aspecten menen wij dat deze voldoende doordacht dienen te zijn teneinde een brede maatschappelijke acceptatie van de benodigde biometrische systemen te ondersteunen. Bij TNO bestaat op dit punt geen expertise en verwezen wordt naar het werk van Prins e.a. [2] en Grijpink [3], het recente rapport van de Registratiekamer [11] en §3.1.1 van dit rapport. Overigens zijn deze juridische aspecten onafhankelijk van de toegepaste biometrische techniek. Juridische aspecten vormen daarom geen beoordelingscriterium.

2.8 Eigenschappen en gebruik van de apparatuur

De vereiste eigenschappen van de apparatuur worden grotendeels bepaald door het toepassingsgebied. Wanneer de biometrische apparatuur geplaatst dient te worden bij reeds in gebruik zijnde apparatuur, kan plaatsgebrek al gauw een rol spelen. Een voorbeeld is de reeds beperkte ruimte op de balie van de marechaussee bij de grenscontrole. Mogelijkheid tot integratie van de biometrische apparatuur/software met een reeds op de werkplek aanwezige PC lijkt daar een voorwaarde. Zoals in §2.3 reeds is uiteengezet, verdient biometrische apparatuur die geen actief handelen van de gebruiker vereist de sterke voorkeur in de toepassing 'look-alikes'.
Geheel andere apparaat-eigenschappen worden vereist in de toepassingsgebieden publieke kiosk en Privé PC. Een voorlopig overzicht van typische apparaat-eigenschappen vereist voor de verschillende toepassingsgebieden is in tabel 6 gegeven.

Tabel 6 - Eigenschappen van biometrische apparatuur

Toepassingsgebied	Eigenschappen
'look-alikes' (begeleid)	• beperkte grootte • hoge kwaliteit, dus relatief hoge prijs • operabel met bestaande PC • geen actieve handeling van gebruiker vereist • API
Publieke kiosk (semi-begeleid)	• grootte niet van direct belang • hoge kwaliteit, dus relatief hoge prijs • foolproof • bestand tegen vandalisme (evt. contactloos) • detectie van "leven en welzijn" • geen actieve handeling van gebruiker vereist • API
Privé PC (niet begeleid)	• zeer klein, eventueel integreerbaar in PC • zeer goedkoop • zeer duurzaam, geen onderhoud nodig • foolproof • beveiligd tegen sabotage • detectie van "leven en welzijn"

Status van Application Programming Interfaces (APIs)

De status van Application Programming Interfaces (API's) voor de verscheidenheid van biometrische apparatuur is van belang teneinde een 'plug-and-play' functionaliteit van verschillende biometrische technieken te kunnen garanderen. De ontwikkeling van API's vindt plaats onder de vleugels van het BioAPI Consortium. Het BioAPI Consortium formuleert haar missie als volgt [12]:
The BioAPI Consortium was formed to develop a widely available and widely accepted API that will serve for various biometric technologies.

The intent is to:
- Work with industry biometric solution developers, software developers, and system integrators to leverage existing standards to facilitate easy adoption and implementation.
- Develop an OS independent standard.
- Make the API biometric independent.

Begin 1999 kwamen de spelers achter de belangrijkste API's - BioAPI, HAAPI and BAPI - overeen hun inspanningen te bundelen in het voordeel van een complexe, multifunctionele API onder de paraplu van BioAPI. De ontwikkeling is in het stadium van onderhandelingen en het nemen van beslissingen. Aan de ontwikkeling wordt door zesendertig bedrijven deelgenomen [13]. Het ziet er naar uit dat de ontwikkeling van een standaard API nog een aantal jaren te gaan heeft.

2.9 Financiële aspecten

De financiële aspecten die een rol spelen bij de aanschaf en implementatie van (biometrische) systemen zijn, zoals vrijwel alle beoordelingscriteria, afhankelijk van het toepassingsgebied, in tabel 6 is deze afhankelijkheid weergegeven. Belangrijke aspecten zijn de volgende:
- Prijs per biometrische eenheid
- Aantal biometrische eenheden
- Commerciële verkrijgbaarheid
- Bijkomende kosten
    - voorbereidingskosten
    - implementatiekosten
    - ontwikkelingskosten
    - voorlichting
    - onderhoud
    - verzekeringskosten

Over de bijkomende kosten kan in dit stadium van het onderzoek geen uitspraak worden gedaan. Het onderzoek zal zich daarom beperken tot de prijscategorie en de commerciële verkrijgbaarheid als beoordelingsmaatstaf.

3 Vraaggesprekken

Teneinde verschillende beoordelingscriteria, zoals omschreven in hoofdstuk 2, te toetsen en teneinde na te gaan wat deskundigen op het gebied van biometrie als kritische succesfactoren beschouwen voor grootschalige toepassing van biometrie, is een aantal vraaggesprekken met deskundigen gevoerd. In appendix 1 is een lijst van ondervraagden gegeven. Een korte samenvatting van de punten van bespreking is in appendix 2 gegeven. Niet alle onderwerpen zijn met alle deskundigen doorgenomen, het gesprek is steeds beperkt tot de specifieke deskundigheid van de ondervraagde. Met name waar de ondervraagden blijk gaven van een bijzondere visie, of waar inzicht kon worden gegeven in grootschalige toepassingen (meer dan 1 miljoen gebruikers) wordt dit hieronder in meer detail besproken.

3.1 Resultaten van de vraaggesprekken

3.1.1 juridische aspecten

Vanuit juridisch oogpunt zijn er geen strikte argumenten aan te dragen die het toepassen van biometrie verhinderen. De relevante wetgeving is te vinden in zowel de grondwet als de Wet Persoons Registratie (WPR). Wel stelt de WPR dat de opgeslagen templates uniek moeten zijn en dat het gebruik van de templates doelgebonden moet zijn.
Het gebruik van biometrie, zoals voorgesteld door BZK, zal in de betreffende visie, identiteitsfraude niet oplossen. Het voorzien van reisdocumenten van een biometrische functie is een veel te zwaar middel en dit zal meer problemen veroorzaken dan oplossen [3] (zie ook hoofdstuk 2.2, 'fall-back' procedures).
Slechts anonieme biometrie kan op grote schaal worden toegepast. Alleen een ketenbenadering, gebaseerd op anonieme biometrie, waarbij slechts aan de basis de juiste identiteit wordt vastgesteld en verder in de keten alleen wordt vastgesteld of de houder van het document de rechtmatige houder is, kan de problematiek rond de identiteitsfraude effectief oplossen [3].
Een splitsing van functies is volgens de betreffende deskundige noodzakelijk:

1. Reisdocumenten gepersonaliseerd maar zonder biometrie.
2. Een anonieme stadspas met biometrie.

De uitgifte van reisdocumenten dient plaats te vinden middels de stadspas. De burgerlijke stand kan bij aanbieden van de stadspas via het persoonsnummer een identificatie uitvoeren.

De uiterste zorgvuldigheid is in de betreffende visie noodzakelijk bij de eerste uitgifte van documenten. De huidige identiteitsketen in Nederland blijkt talloze onvolkomenheden te vertonen en een ketenbrede verbeteringsoperatie is daarom volgens de betreffende deskundige wenselijk voordat electronische identiteiten ons door de vingers glippen [3].
De invoering van biometrie in Nederland dient te worden gerealiseerd in het kader van internationale samenwerking en overleg.

In een ander systeemconcept wordt door een deskundige de nadruk gelegd op de behoefte aan de functionaliteit om elektronisch aan het maatschappelijke verkeer deel te nemen in de relatie tussen overheid en burger. Eén van de mogelijkheden is het 'digitale paspoort'. Dit digitale paspoort zal de volgende kenmerken moeten hebben:

⇒ drager van persoonsgegevens, aangebracht volgens een gecontroleerd proces (bron bijv. GBA),
⇒ biometrie om de identiteit van de houder vast te stellen,
⇒ voorziening voor een digitale handtekening.

Deze drie elementen, in combinatie met een 'secure token', kunnen goed gebruikt worden in het maatschappelijk (berichten) verkeer. Biometrie kan worden gebruikt om de diensten aan te spreken, als "luxe PIN-code" om functionaliteiten te ontsluiten. Biometrie moet niet worden gebruikt in combinatie met opslag in een database (centraal dan wel decentraal), maar primair als verificatie van authenticiteit van de gebruiker.

3.1.2 beveiliging

Met betrekking tot het niveau van de beveiliging voor de verschillende toepassingsgebieden zijn alle deskundigen het eens. Ook bestaat eensgezindheid over de noodzaak een adequate identificatie ten grondslag te leggen aan de uitgifte van identiteitsdocumenten. Twee van de deskundigen zijn van mening dat dit in Nederland nog steeds niet goed is geregeld. Meervoudige identiteiten komen nog veel voor.
Vrijwel alle deskundigen zijn van mening dat een FRR omstreeks 1% een goede prestatie is, die vooralsnog niet sterk verbeterd zal worden.
Een van de deskundigen meent echter dat er een toenemende verbetering bestaat en dat dit binnenkort geen probleem meer zal zijn. Een acceptabele FRR lijkt deze deskundige een waarde van 1 : 1000 tot 1 : 500, bij kritische toepassingen zal dit echter niet voldoende zijn en is biometrie geen optie.
Naar de mening van een andere deskundige mag de FRR enige procenten bedragen, wanneer de organisatie ('fall-back' procedure) maar in orde is. Overigens meent deze deskundige dat een FRR van 1 : 200 bij de IrisSan haalbaar is. Travel pass biometrie voor snelle grenspassage van reizigers zal naar zijn mening altijd begeleid moeten zijn.

Met betrekking tot het adequaat functioneren van 'fall-back' procedures wordt aangevoerd dat deze procedure van het grootste belang is voor grote open toepassingen en dat men een onafhankelijke 'fall-back' biometrie zou kunnen invoeren om deze te beveiligen tegen de identiteitsfraude die thans mogelijk wordt gemaakt door menselijk falen. In zo'n 'of-of' procedure, waarbij de gebruiker na een reject in de 'fall-back' procedure de kans krijgt een onafhankelijke biometrie te tonen, zal de totale FRR van beide biometrische technieken het product zijn van beide afzonderlijke FRRs.

Over de toepassing van een detectie van "leven en welzijn" op het biometrische kenmerk is niet zeer veel bekend. Enkele deskundigen twijfelen of deze detectie in alle gevallen werkzaam zal zijn en misleiding kan voorkomen. Een der deskundigen geeft aan dat het moeilijk zal zijn een adequate test op "leven en welzijn" uit te voeren met vingerbiometrie. Een ander wijst erop dat deze detectie steeds minder vaak wordt geïmplementeerd, vermoedelijk omdat het niet noodzakelijk wordt geacht. Een derde deskundige geeft aan dat adequate detectie van "leven en welzijn" van het grootste belang is.

3.1.3 toepasbaarheid en acceptatie

Met betrekking tot het uniek zijn van biometrische kenmerken wordt door een deskundige opgemerkt dat dit afhangt van het aantal beschrijfbare en meetbare typica (zie sectie 2.4). Gezichtsherkenning is hierom volgens deze deskundige geen goede biometrie.

Over de veroudering van biometrische kenmerken wordt door verschillende experts opgemerkt dat irisherkenning vermoedelijk het beste zal scoren en dat vingerpatronen een goede tweede zullen vormen. Gelaatstrekken en handvorm zijn veel minder stabiel. De mogelijkheid van regelmatige updating is voor iedere biometrische techniek mogelijk, toepassing zal alleen plaatsvinden voor kenmerken met een duidelijke atrofie.
Over het discriminerend vermogen van biometrische apparatuur op lange termijn, d.w.z. de spreiding van de foutpercentages in de tijd werd door geen van de deskundigen iets aangevoerd.

Een deskundige meent dat vingerbiometrie in Nederland nu zeker geaccepteerd zal worden; de markt is er rijp voor.

Een andere deskundige meent dat oogbiometrie weinig aanvaardbaar zal zijn, vingerbiometrie, handgeometrie, gezichtsherkenning en stemverificatie zullen acceptabel zijn.

Volgens weer een andere deskundige is acceptatie van biometrie is geen probleem, het publiek vindt het leuk, zeker als vervanging van een PIN-code. Deze deskundige deelt mee dat uit een kwantitatief onderzoek m.b.t. de acceptatie van biometrie in relatie met overheidsdiensten blijkt dat hier geen obstakels meer mogen verwacht.

De volgende inschatting (tabel 7) werd door een der deskundigen gemaakt van de commerciële beschikbaarheid en volwassenheid van verschillende biometrische technieken.

Tabel 7 - commerciële beschikbaarheid en proven technology*)

biometrie	Commercieel	proven technology	opmerkingen
Iris	X	x	Nog in vroeg stadium
Retina			Weinig of geen activiteit waarneembaar
Handgeometrie	X	x	
Handaderpatroon (Veincheck)			Nog in ontwikkeling
Vingergeometrie	X	x	
Vingerpatroonscaner	X	x	
Oorgeometrie			Nog in ontwikkeling
Gezichtsherkenning	X	x	Er wordt nog steeds verbeterd
3D gezichtsherkenning			Neuro Dynamincs, semi-commercieel
Geurkarakteristiek			Nog in ontwikkeling
Stemherkenning	X		Nog te weinig toegepast
Dynamische handtekening	X		
Dynamiek toetsaanslag			Er bestaat 1 systeem

*)Vlgs. één der geraadpleegde deskundigen

3.1.4 grootschalige, operationele toepassingen

Gevraagd naar voorbeelden van grootschalige toepassing van biometrie wijst een aantal ondervraagde deskundigen naar het Tass project, een social security card met vingertemplate, in Andalusië, Spanje, dat in 1994 werd geïntroduceerd. Het blijkt echter dat het project niet naar geheel Spanje zal worden uitgebreid (Btt 6,10). Niettemin zijn er drie miljoen kaarten gedistribueerd, zodat van een grootschalig project sprake lijkt te zijn. Een delegatie van BZK heeft zich medio 1999 ter plaatse op de hoogte gesteld van de status

van het project. Uit een vraaggesprek met een der delegatieleden is gebleken dat de frequentie van het gebruik van de kaart door het publiek tegenvalt. De organisatie overweegt daarom studenten in te zetten als begeleider van de biometrische kiosken. De situatie is thans zo dat de kiosken nabij een loket staan en het publiek zich liever tot het loket wendt. Het laat zich aanzien dat de toepassing van biometrie voor de gebruiker geen duidelijke voordelen biedt of dat deze zich van mogelijke voordelen niet bewust is.
Een recent overzicht van grootschalige civiele toepassingen van biometrie, met miljoenen gebruikers, is gegeven in tabel 8.

Tabel 8 – grootschalige civiele toepassingen van biometrie*)

Land	Techniek	Functie	Aanvang	Aantal gebruikers	Status
Argentinië	AFIS	Nationale ID-card	eind 1999	>50 miljoen	gestart
Bolivia	vinger	Nationale ID en stemregistratie project	1998	4,5 - 7 miljoen	pilot
Botswana	vinger	Identificatiesysteem ter voorkoming van meervoudige paspoort aanvragen	1996	-	gestart
Cambodja	vinger	Nationale ID, gezondheidszorgkaart, stemmen en grensverkeer	1999	< 8 miljoen	gestart
Colombia	AFIS	Elimineren stem- en steunfraude	1998	25 miljoen	gestart
Costa Rica	vinger	Stemregistratiekaart	1998	3,4 miljoen	gestart
Domin. Rep.	vinger	Nationale ID-card	1998	< 5 miljoen	gestart
Honduras	vinger	Nationale ID-card	1998	> 4,1 miljoen	gestart
Libanon	AFIS	Nationale ID-card	1997	> 4 miljoen	gestart
Nigeria	AFIS	Civiele registratie	-	54 miljoen	gestart
Panama	vinger	Nationale ID-card en stemregistratie	1999	< 3 miljoen	gestart
Peru	vinger	Civiele registratiekaart	1998	< 12 miljoen	gestart
Filippijnen	AFIS	Bestrijding fraude volksverzekering	1998	35 miljoen in 2004	gestart
Zuid-Afrika	AFIS	Garanderen identiteit voor alle civiele zaken, ook toegankelijk voor politie	1999	> 45 miljoen	hangend
Taiwan	AFIS	Nationale ID-card	2001	< 20 miljoen	hangend

*) Bron: Biometric Technology Today, vol. 6, no. 9, februari 1999.

Opvallend in dit overzicht is dat de meeste toepassingen in Latijns Amerika en het Verre Oosten zijn gestart en geen enkele toepassing in Europa. Alle toepassingen zijn recentelijk gestart en het invoeren van miljoenen gebruikers kan jaren duren. Voorts is de toepassing van AFIS op een populatie van tientallen miljoenen, vanwege de grootschaligheid, een zeer gecompliceerde zaak, op de grens van de mogelijkheden die de hedendaagse AFIS systemen bieden [14]. In hoeverre deze toepassingen al of niet succesvol zijn kan dus eerst worden bepaald wanneer ze op de geplande volledige schaal functioneren. Grootschalige, operationele toepassingen bestaan momenteel dus nog niet.
Opvallend is ook dat in veel gevallen AFIS als biometrie wordt toegepast, waarbij meerdere vingerafdrukken ongecodeerd worden opgeslagen in een centrale database. Dit kan een uiterst effectief middel zijn om een adequaat landelijk identificatiesysteem te realiseren. Het is echter de vraag of een dergelijke toepassing in Nederland haalbaar is [2]. Waar geen AFIS wordt ingezet, wordt vingerbiometrie met opslag van template gebruikt. In alle gevallen worden de grootschalige civiele toepassingen dus gebaseerd op het patroon van vingerlijnen.

De doelstelling van deze civiele systemen is steeds een biometrisch identificatiesysteem en enige voorzichtigheid met het trekken van conclusies m.b.t. geprojecteerde grootschalige verificatiesystemen is daarom geboden.

Biometrie wordt ook toegepast als basis voor identificatiesystemen in sociale programma's teneinde meervoudige uitkeringen aan een zelfde persoon met meerdere valse identiteiten te voorkomen. De schaal van deze toepassingen is middelgroot, variërend van enkele tienduizenden tot honderdduizenden gebruikers, en in uitzonderlijke gevallen is de schaal zelfs groot, met miljoenen gebruikers. In vrijwel alle gevallen zijn AFIS en vingerbiometrie hier de toegepaste biometrische technieken [Btt 7,1]. De meeste toepassingen zijn tamelijk recent - tweede helft negentiger jaren - maar gezien de geringere omvang zijn vele toepassingen thans reeds operationeel geworden. Het succes van deze toepassingen berust op een aantal factoren. Allereerst vormt de detectie van meervoudige identiteiten de gewenste beveiliging. Het blote feit dat een dergelijk systeem in werking is heeft echter tevens tengevolge dat potentiële fraudeurs worden afgeschrikt. Hoewel deze laatste bijdrage aan de beveiliging niet meetbaar is, wordt algemeen aangenomen dat deze substantieel is. Bij deze toepassingen zijn de biometrische systemen begeleid, zodat misbruik en bedrog geen kans maken. De gebruiker zal dus coöperatief zijn, daar het resultaat voor hem kritisch is (gebruikersprofiel 4, 6) hetgeen het goede functioneren van het systeem zal bevorderen.

De tientallen middel- en grootschalige civiele toepassingen van biometrie zijn vrijwel zonder uitzondering alle gebaseerd op het vingerlijnenpatroon. Dit maakt wel duidelijk dat de vereiste uniciteit van het biometrische kenmerk vooralsnog slechts wordt toegekend aan het vingerlijnenpatroon, dat dit vooral dankt aan de duidelijke beschrijfbaarheid en meetbaarheid van tientallen duidelijk onderscheiden typica (§2.4). Een serieuze mededinger in dit opzicht is irisbiometrie. Irisbiometrie heeft echter nog niet het stadium van volwassenheid bereikt van vingerbiometrie, hoewel dit naar verwachting niet lang meer zal duren. Irisbiometrie is vooralsnog aanzienlijk duurder dan vingerbiometrie en dit prijsverschil zal mogelijk een belangrijke rol spelen wanneer de apparatuur op veel locaties dient te worden opgesteld.

3.1.5 kritische succesfactoren

Gevraagd naar de kritische succesfactoren voor grootschalige toepassingen van biometrie wordt door de deskundigen op aandachtspunten in een viertal gebieden gewezen:

1. Acceptatie door de gebruiker
2. Betrouwbaarheid van het biometrische systeem
3. Organisatie
4. Technologie

In het volgende zijn de verschillende zienswijzen van de deskundigen tot een geheel samengevoegd.

<u>Acceptatie door de gebruiker</u>

De toepassing dient voor iedereen beschikbaar, bereikbaar en betaalbaar zijn.

De toepassing dient voor de gebruiker zinvol en nuttig zijn en als een duidelijke verbetering op de bestaande situatie te worden ervaren. Integratie van biometrie in het reisdocument dient zonder veel ophef te geschieden als middel tot bestrijding van fraude. Een daaropvolgende offspin van dienstverlening in de burgermaatschappij zal daarop geleidelijk geaccepteerd worden.

De noodzakelijkheid dient door de gebruiker 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.
Voorts dient een hoge mate van gebruiksgemak te worden geboden, door ergonomische vormgeving en een omgeving waarin het gebruik eenvoudig en aantrekkelijk wordt gemaakt en additionele, externe druk wordt voorkomen. Het vertrouwen van de potentiële gebruiker in de toepassing dient te worden gewekt door een degelijke uitstraling.

Betrouwbaarheid
De biometrische apparatuur moet foolproof zijn. En storingsvrije werking is noodzakelijk, daar anders de drempelinstelling avn de apparatuur door het bedienend- of servicepersoneel zal worden verlaagd teineinde de false reject rate te verlagen. Mogelijk een kan een combinatie van biometrische systemen worden gebruikt om de betrouwbaarheid te vergroten (zg. multi-modal recognition, bijv. een combinatie van gezichts- en stemherkenning).
De biometrische techniek moet onafhankelijk zijn van variabelen als bloeddruk, manier van aanleggen, beschadiging, groei, littekens, enz. Ook de beschikbaarheid van het biometrische kenmerk dient voldoende te zijn; er moet altijd een alternatief zijn (zoals een andere vinger).
De verificatieprocedure dient zo betrouwbaar mogelijk te zijn door adequate begeleiding.

Organisatie
Het gebruik van elektronische documenten voor dienstverlening op ieder plek wordt gezien als de toekomst. In een diensteneconomie moet daarom ook de overheid deze diensten elektronisch toegankelijk maken. Als voorbeeld wordt genoemd het integreren van diensten door uitkeringsinstanties. De overheid dient de mogelijkheid tot biometrische verificatie te bieden. De verschillende dienstverleners kunnen vervolgens bepalen of ze van deze functionaliteit gebruik willen maken. Het laatste woord is dan aan de gebruiker, de houder van de kaart, die zal beslissen of hij van deze vorm van dienstverlening gebruik wil maken. Het lijkt realistisch om deze vorm van dienstverlening binnen afzienbare tijd in te voeren, echter eerst na adequaat testen van de systemen in verschillende situaties met verschillende dienstverleners en gebruikers. Het is onverstandig over te gaan tot landelijke invoering voordat aan alle randvoorwaarden is voldaan. Wanneer de invoering vroegtijdig en onvoldoende voorbereid plaats vindt en daardoor mislukt, is de kans waarschijnlijk verkeken de fout binnen afzienbare tijd te herstellen. Dit traject zal zeker drie jaar duren, maar vijf jaar is een niet onrealistische termijn.

In het bijzonder wordt de aandacht erop gevestigd dat de organisatorische basis voor het systeem geheel in orde dient te zijn: een adequate identificatie van de gebruikers dient aan het systeem ten grondslag te liggen.

De correcte invoer van zeer grote aantallen gebruikers onder efficiënte begeleiding is van bijzonder belang. Er kan niet alleen op de techniek worden vertrouwd, zijn mensen bij betrokken en adequate procedures zullen het gebruik moeten ondersteunen.

Technologie

Biometrie is het meest betrouwbare middel voor persoonsauthenticatie, maar men moet er niet teveel van verwachten. Ook moet niet teveel worden verwacht van multifunctionele toepassingen, de technologie is nog niet ver genoeg gevorderd. Houdt het daarom zo eenvoudig mogelijk.

Er moet rekening mee worden gehouden dat biometrie op zichzelf niet zal werken, zeker niet bij thuisgebruik. Een combinatie van smart card, PKI en Biometrie - in een verificatieketen - zal een adequate werking moeten verzekeren.

De apparatuur dient handzaam te zijn, mogelijkheid tot plug-and-play en integratie van hardware en software in bestaande platforms. Aandacht dient besteed te worden aan standaardisatie van de apparatuur.

De apparatuur moet ook goedkoop zijn, maar dit is wel een relatief gegeven en een kosten-baten analyse dient hierin nader inzicht te geven. Tenslotte dient te worden overwogen in hoeverre nieuwe ontwikkelingen worden verwacht, en of deze dan probleemloos kunnen worden ingevoerd, of dat men aan de oude technologie vast zit.

4 Inventarisatie, selectie en beoordeling van biometrische technieken

De belangrijkste biometrische technieken zijn geïnventariseerd. Deze biometrische technieken worden vervolgens beoordeeld aan de hand van de vastgestelde beoordelingscriteria. Op basis hiervan wordt een uitspraak gedaan over de toepasbaarheid van de verschillende biometrische technieken in de betrokken grootschalige civiele toepassingsgebieden van de reisdocumenten. Geen enkel beoordelingscriterium is op zich voldoende om een definitieve keuze te rechtvaardigen. Het is de weging van de gezamenlijke criteria die een definitieve uitspraak mogelijk maakt.

4.1 Inventarisatie en selectie van biometrische technieken

Momenteel wordt een variëteit aan biometrische kenmerken gebruikt voor verificatie en identificatie of de technieken zijn daarvoor in ontwikkeling. Er wordt een onderscheid gemaakt tussen fysieke kenmerken en gedragskenmerken. In tabel 9 is van de belangrijkste van beide types biometrische kenmerken een overzicht gegeven, hierin zijn niet alle voorkomende biometrische kenmerken opgenomen. Relatief nieuwe biometrische kenmerken zijn bijvoorbeeld de manier van lopen, lipgeometrie en nagelbedpatronen. De biometrische technieken die op deze nieuwe kenmerken berusten, zijn alle nog in het onderzoeksstadium. Hiernaast is nog sprake van een gevestigde laboratoriumtechniek voor identificatie van personen: DNA analyse. Deze laatste identificatietechniek vereist een laboratoriumtest van ten minste tien minuten, en is dus nog ongeschikt als verificatiemethode.

4.1.1 commerciële beschikbaarheid

Sommige van de in tabel 9 genoemde technieken staan nog in de kinderschoenen, andere zijn deze reeds ontgroeid en hebben succesvolle commerciële toepassingen gevonden.

Tabel 9 – Status biometrische technieken*)

Fysieke kenmerken	Status en aantal producenten		Gedragskenmerken	Status en aantal producenten	
Gezichtsherkenning	Commercieel	16	Stemkarakteristiek	commercieel	27
Gelaatswarmtepatroon	bèta testversie	1	Dynamiek handtekening	commercieel	14
Irispatroon	Commercieel	3	Dynamiek toetsaanslag	commercieel	1
Retina aderpatroon	Commercieel	1			
Oorgeometrie	research stadium	n.v.t.			
Vingerlijnenpatroon	Commercieel	circa 100			
Handpalmlijnenpatroon	prototype	3			
Handgeometrie	Commercieel	2			
Vingergeometrie	Commercieel	1			
Handaderpatroon	prototype	1			
Polsaderpatroon	gepland	n.v.t.			
Geurkarakteristiek	research stadium	n.v.t.			

*) Bronnen: Btt vol. 7, nr. 4 (1999) hand measuring systems; Btt vol. 7, nr. 2 (1999) signature verification systems, Btt vol. 7, nr. 2 (1999) speaker verification systems, Btt vol. 6,nr. 10 (1998) finger technologies; Btt vol. 6, nr. 6 (1998): ear, eye, gait, keystroke, lip, and nailbed biometrics, Btt vol. 6, nr. 5 (1998) face recognition.

Een eerste selectie op de commerciële verkrijgbaarheid en het aantal producenten (meer dan twee vereist) laat de volgende biometrische technieken over voor nadere beschouwing:

- gezichtsherkenning
- irispatroon
- vingerlijnenpatroon
- stemkarakteristiek
- dynamiek van de handtekening.

4.1.2 vandalisme

Wanneer vervolgens het beoordelingscriterium bestendigheid tegen vandalisme in aanmerking wordt genomen, dan blijkt dit criterium slechts relevant voor het toepassingsgebied kiosk in openbare ruimte (§2.3). De kans op vandalisme is gering in toepassingsgebieden waar begeleiding aanwezig is en deze kans is in het geheel niet relevant voor het toepassingsgebied privé PC. Het verdient aanbeveling voor onbegeleide of semi-begeleide toepassingen geen biometrische technieken te gebruiken waarbij het publiek direct contact met de apparatuur heeft. In tabel 10 is een overzicht gegeven van de bruikbaarheid van de resterende biometrische technieken op grond van deze overweging.

Tabel 10 - toepasbaarheid met het oog op vandalisme

Biometrie	'look-alikes'	kiosk	privé PC
gezichtsherkenning	+	+	+
irisherkenning	+	+	+
vingerpatroonherkenning	+	-	+
stemherkenning	+	+	+
dynamische handtekening	+	-	+

4.1.3 eigenschappen van het biometrische kenmerk

In §2.4 zijn de verschillende eigenschappen van biometrische kenmerken besproken, die in het kader van het onderzoek van belang zijn. Deze kenmerken zijn gevoeligheid voor fraude door het aanbieden van imitaties e.d., de uniciteit, de duurzaamheid, de beschikbaarheid, de toegankelijkheid en de acceptatie van het biometrische kenmerk. Hieronder worden deze eigenschappen nader beschouwd voor gelaatstrekken, irispatroon, vingerlijnenpatroon, stemkarakteristiek en dynamiek van de handtekening.

Identiteitsfraude - Identiteitsfraude door het aanbieden van imitaties van kenmerken, e.d. maakt weinig of geen kans bij begeleide toepassingen. Waar geen begeleiding bestaat of slechts semi-begeleiding dient de eis te worden gesteld dat dergelijke identiteitsfraude voorkomen wordt door een adequate detectie van het levend zijn van het biometrische kenmerk.

In hoeverre de verschillende biometrische technieken aan deze eis kunnen voldoen is niet met zekerheid te zeggen. Naar verluidt wordt het irispatroon op kleine onwillekeurige bewegingen van de pupil gecontroleerd, hetgeen een goede methode van beveiliging zou zijn. Een goede detectie bij vingers lijkt lastiger. Veelal maken droge vingers geen goed contact met de apparatuur, controle op de kleur van de vinger dient met een ruim scala van kleuren rekening te houden en controle op warmte dient zeer ruim te zijn daar de temperatuur van extremiteiten zeer uiteen kan lopen. Hiernaast speelt nog een rol dat een afgietsel van een vingerpatroon gemakkelijk kan worden gemaakt en onopvallend aan de biometrische apparatuur kan worden aangeboden, zelfs wanneer toezicht aanwezig is.

Producenten van apparatuur voor de herkenning van de stemkarakteristiek beweren dat deze geen imitaties op een band accepteert. De dynamiek van de handtekening is een geval apart, een test op leven is in dit geval uiteraard niet zinvol. Het is echter denkbaar dat iemand het ritme gadeslaat, waarmee een handtekening wordt gezet, en dit succesvol imiteert. Hiertegen is uiteraard geen detectie mogelijk.
Het verdient aanbeveling een nader onderzoek in te stellen naar de wijze waarop de verdediging tegen imitaties bij de verschillende biometrische technieken is ingericht en in hoeverre deze verdediging effectief mag worden geacht.

Acceptatie van het gebruik - Over de acceptatie van het gebruik van een bepaald biometrisch kenmerk valt weinig definitiefs te zeggen. Bij publieke toepassingen zullen contactloze methoden mogelijk beter scoren dan methoden waarbij fysiek contact met de apparatuur moet worden gemaakt, omdat deze naar verwachting als minder opdringerig zullen worden ervaren.
Verwacht mag worden dat gezichtsherkenning op weinig weerstand zal stuiten daar dit in het maatschappelijk verkeer reeds gebruikelijk is. Hetzelfde kan worden verondersteld van stemherkenning en het plaatsen van een handtekening. Het is voorts de vraag in hoeverre de gebruiker in deze tijd nog bezwaar zal hebben tegen het plaatsen van een vinger op een detector in verband met een associatie met criminaliteit, eerder zullen waarschijnlijk hygiënische bezwaren een rol spelen. Slechts weinigen zullen bezwaar maken tegen irisherkenning op grond van de vrees daarmee het lijden aan eventuele ziektes prijs te geven. De afstand van het oog tot de apparatuur is tevens zo groot (circa 75 cm) dat dit in het algemeen niet als bedreigend voor het oog zal worden ervaren.
De uiteindelijke acceptatie van een biometrische techniek zal naar verwachting voornamelijk afhankelijk zijn van effectieve voorlichting, de gewaarwording van het nut van het gebruik en persoonlijke voordelen.

Uniciteit, duurzaamheid, beschikbaarheid en toegankelijkheid - Over deze resterende eigenschappen van biometrische kenmerken kan in kwalitatieve zin een uitspraak worden gedaan.
Over de uniciteit kan iets worden gezegd op grond van het aantal beschrijfbare en meetbare typica dat een biometrisch kenmerk biedt.
De duurzaamheid van gedragskenmerken is in het algemeen geringer dan die van fysieke kenmerken. Van deze laatste is het irispatroon verreweg het meest duurzaam. Het vingerlijnenpatroon - als patroon op zich - is in principe zeer duurzaam, maar het patroon is meer blootgesteld aan beschadiging en slijtage.
Over de beschikbaarheid van een biometrisch kenmerk kan een uitspraak worden gedaan op grond van het aantal onafhankelijke kenmerken dat voor controle beschikbaar is.
De toegankelijkheid van deze biometrische kenmerken is hoog voor zover ze contactloos zijn. De toegankelijkheid van het vingerlijnenpatroon is hier de uitzondering, daar het op de juiste wijze plaatsen van de vinger in de praktijk een probleem kan zijn, terwijl tevens te droge of juist te natte vingers regelmatig voorkomen.
In tabel 11 is een overzicht gegeven van deze eigenschappen van de besproken biometrische kenmerken. Uit het overzicht blijkt dat irispatroon en vingerlijnenpatroon gemiddeld verreweg het hoogst scoren.

Tabel 11 - het biometrische kenmerk				
Biometrie	**Uniciteit**	**duurzaamheid**	**beschikbaarheid**	**toegankelijkheid**
Gezichtsherkenning	gering/matig	matig	gering	hoog
Irispatroon	zeer hoog	zeer hoog	voldoende	hoog
Vingerlijnenpatroon	zeer hoog	voldoende	zeer hoog	matig
Stemkarakteristiek	?	gering	gering	hoog
Dynamiek handtekening	matig/voldoende	gering	gering	hoog

4.1.4 betrouwbaarheid en 'proven technology'

Het feit dat de vijf resterende biometrische technieken commercieel verkrijgbaar zijn en alle drie of meer producenten kennen, betekent reeds dat een zekere mate van volwassenheid zou mogen worden aangenomen. Niettemin kent een der geraadpleegde deskundigen dit predikaat niet toe aan de beide gedragskenmerken stemherkenning en dynamische handtekening en meent deze zelfde deskundige dat de irisherkenning nog maar net in het volwassen stadium is beland (zie tabel 7). In tabel 12 zijn voor de resterende biometrische technieken de opmerkingen van deze deskundige nog eens op een rijtje gezet. Vooralsnog is vingerpatroonherkenning de biometrische techniek die zich onderscheidt door toepassingen op grote schaal.

Tabel 12 – Proven technology*)		
biometrie	**proven technology**	**opmerkingen**
Gezichtsherkenning	+	Er wordt nog steeds verbeterd
Irisherkenning	+	Nog in vroeg stadium
Vingerpatroonherkenning	+	
Stemherkenning		Nog te weinig toegepast
Dynamische handtekening		

*)Vlgs. één der geraadpleegde deskundigen (vergelijk tabel 7)

In §2.5 is een aantal factoren genoemd die invloed hebben op de betrouwbaarheid van een biometrische techniek: de foutpercentages FAR, FRR en FTE, het discriminerend vermogen op lange termijn, MTBF (mean time between failure) en MTTR (mean time to repair), en de aanwezigheid van een test op "leven en welzijn". Van geen van deze factoren is momenteel voldoende bekend om een zinvol onderscheid te kunnen maken tussen de resterende biometrische technieken. Wel kan worden verwacht dat het discriminerend vermogen op lange termijn voor irisherkenning het grootst zal zijn en dat vingerpatroonherkenning in dit opzicht een goede tweede zal zijn. Beide biometrische kenmerken vertonen immers de hoogste mate van uniciteit en zijn in de tijd het meest constant (tabel 11).
Vooralsnog wordt aangenomen dat technologische volwassenheid en betrouwbaarheid voornamelijk het kenmerk zijn van gezichts-, irispatroon- en vingerpatroonherkenning.

4.1.5 maatschappelijke acceptatie

In §2.7 is aangevoerd dat maatschappelijke acceptatie van biometrie samenhangt met drie factoren: (1) de techniek, (2) de toepassing en (3) het psychologisch profiel van de gebruikersgroep. De toepassing en het profiel van de gebruikersgroep vormen echter geen factoren die onderscheid mogelijk maken naar maatschappelijke acceptatie van de biometrische techniek.

In §4.1.3 is met betrekking tot de maatschappelijke acceptatie het een en ander gesteld over de resterende biometrische technieken. Een definitieve uitspraak over de acceptatie van de verschillende biometrische technieken blijkt niet mogelijk. Contactloze methoden zullen naar verwachting wat beter scoren dan methoden waarbij fysiek contact met de apparatuur moet worden gemaakt. Hier hebben gezichts-, iris- en stemherkenning een voordeel boven vingerpatroonherkenning. Het plaatsen van een handtekening - onder zeer verschillende omstandigheden - is maatschappelijk geaccepteerd en voor de biometrische techniek van de dynamische handtekening mag daarom geen afwijzende houding verwacht worden. De uiteindelijke acceptatie van een biometrische techniek zal echter, naar verwacht mag worden, voornamelijk afhankelijk zijn van effectieve voorlichting, de publieke gewaarwording van het nut van het gebruik en het bestaan van persoonlijke voordelen.

4.1.6 eigenschappen en gebruik van de apparatuur

In §2.8 is een voorlopig overzicht gegeven van de vereiste eigenschappen van biometrische apparatuur en het gebruik ervan voor de verschillende toepassingsgebieden (zie tabel 6). In het volgende worden uit dit overzicht die eigenschappen beschouwd die een beoordelingscriterium kunnen bieden in de keuze van biometrische technieken voor de verschillende toepassingsgebieden.

'Look-alikes' - Tabel 13 geeft een overzicht van de eigenschappen die kunnen dienen als beoordelingscriterium voor de geschiktheid van biometrische apparatuur voor het toepassingsgebied 'look-alikes'. De apparatuur voor irisherkenning heeft aanzienlijke afmetingen, terwijl de dynamische handtekening een redelijk grote plaats vereist waar de gebruiker een handtekening kan plaatsen in het zicht van de controleur. Alleen iris- en gezichtsherkenning vereisen nauwelijks of geen actief handelen van de gebruiker. Op basis van deze criteria zouden alleen gezichtsherkenning en (indien afmeting er niet toe doet) irisherkenning in aanmerking komen voor het toepassingsgebied 'look-alikes'.

Tabel 13 - Geschiktheid biometrische techniek voor toepassing 'look-alikes'

biometrie	Afmeting	passief	geschiktheid
Gezichtsherkenning	Klein	ja	groot
Irisherkenning	Groot	ja	matig
Vingerpatroonherkenning	Klein	nee	gering
Stemherkenning	Klein	nee	gering
Dynamische handtekening	Matig groot	nee	zeer gering

Publieke kiosk - Tabel 14 geeft een overzicht van de eigenschappen die kunnen dienen als beoordelingscriterium voor de geschiktheid van biometrische apparatuur voor het toepassingsgebied publieke kiosk. Er is van uit gegaan dat contactloze passieve technieken meer foolproof zijn dan technieken die een interactie van de gebruiker of contact met de gebruiker vereisen. Contactloze technieken kunnen eveneens beter tegen vandalisme worden beschermd. Op deze gronden lijken iris- en gezichtsherkenning de meest aangewezen biometrische technieken voor dit toepassingsgebied.

Tabel 14 - Geschiktheid biometrische techniek voor toepassing publieke kiosk				
biometrie	**Foolproof**	**contactloos**	**passief**	**geschiktheid**
Gezichtsherkenning	Ja	ja	ja	zeer groot
Irisherkenning	Ja	ja	ja	zeer groot
Vingerpatroonherkenning	Nee	nee	nee	zeer gering
Stemherkenning	Nee	ja	nee	gering
Dynamische handtekening	Nee	nee	nee	zeer gering

Privé PC - Tabel 15 geeft een overzicht van de eigenschappen die kunnen dienen als beoordelingscriterium voor de geschiktheid van biometrische apparatuur voor het toepassingsgebied privé PC. De meeste van de beschouwde biometrische technieken zijn klein. Vingerpatroonherkenning kan in het toetsenbord of de muis worden ingebouwd, de kleine camera die op de monitor wordt geplaatst is reeds gemeengoed, evenals de microfoon die standaard bij veel computers wordt geleverd. Het is niet ondenkbaar dat ook een tablet voor dynamische handtekening naast de computer acceptabel wordt gevonden.

Tabel 15 – geschiktheid biometrische techniek voor toepassing privé PC				
biometrie	**Afmeting**	**foolproof**	**prijs**	**geschiktheid**
Gezichtsherkenning	Klein	ja	laag	hoog
Irisherkenning	Groot	ja	zeer hoog	zeer gering
Vingerpatroonherkenning	Klein	nee	laag	voldoende/hoog
Stemherkenning	Klein	nee	laag	voldoende/hoog
Dynamische handtekening	Matig groot	nee	laag	matig/voldoende

De prijzen van al deze technieken zijn laag genoeg voor dit toepassingsgebied. Irisherkenning is echter zeer duur en moet voor deze toepassing worden uitgesloten. Vingerpatroonherkenning, stemherkenning en dynamische handtekening vereisen een actieve handeling, die constant is in de tijd, van de gebruiker. Wanneer verwacht mag worden dat een thuisgebruiker gemotiveerd en relatief frequent van het systeem gebruik maakt, behoeft dit echter geen nadeel te zijn en het beoordelingscriterium 'foolproof' behoeft dan niet zeer zwaar te wegen. Het zetten van een handtekening die in de tijd constant is, vereist echter concentratie van de gebruiker: veel mensen zijn gewend in haast een snelle versie van hun handtekening te plaatsen die in ritme en pengebruik beduidend afwijkt van de meer nauwkeurige versie die mogelijk is ingevoerd. Deze snelle versie zal dan tot een reject leiden. Het plaatsen van een handtekening heeft echter een uniek voordeel boven andere biometrische technieken: de expliciete betekenis van deze actieve handeling is de intentie van de gebruiker accoord te gaan met hetgeen waarvoor getekend wordt. Dit geeft de dynamische handtekening naast de beveiligende waarde een wettelijke relevantie.
Op grond van deze overwegingen lijken vingerpatroon-, gezichts-, stemherkenning en dynamische handtekening geschikte technieken voor dit toepassingsgebied.
Samenvatting - Samenvattend kan worden gesteld dat, op grond van de eigenschappen en het gebruik van de apparatuur, voor de verschillende toepassingsgebieden zeer verschillende overwegingen gelden voor de keuze van een biometrische techniek. De enige biometrische techniek die - op grond van deze overwegingen - voor alle besproken toepassingsgebieden in aanmerking lijkt te komen is gezichtsherkenning.

4.2 Eindbeoordeling van biometrische technieken

Na de selectie op commerciële beschikbaarheid, resteerden de volgende beoordelingscriteria voor een nadere selectie: weerstand tegen vandalisme, eigenschappen van het biometrisch kenmerk, betrouwbaarheid en 'proven technology', en eigenschappen en gebruik van de apparatuur. De resterende biometrische technieken zijn in de paragrafen 4.1.2 t/m 4.1.6 op deze criteria beoordeeld. In het volgende worden deze beoordelingen samengevat, zodat op basis daarvan een voorlopige keus voor één of meer biometrische technieken kan worden gemaakt voor de verschillende toepassingsgebieden. Met nadruk wordt erop gewezen dat deze samenvatting noodzakelijkerwijs schematisch is, en niet kan worden beoordeeld zonder de toelichtingen op de verschillende beoordelingen in aanmerking te nemen.

4.2.1 toepasbaarheid biometrische technieken

'Look-alikes' - In tabel 16 is de samenvatting gegeven van de verschillende beoordelingen voor het toepassingsgebied 'look-alikes'. Daar de biometrische inspectie begeleid wordt, is de weerstand tegen vandalisme voor dit toepassingsgebied niet relevant. Slechts gezichts-, iris, en vingerpatroonherkenning komen voor nadere beschouwing in aanmerking. Geen van deze biometrische technieken scoort positief op alle beoordelingscriteria. De keuze wordt bepaald door het belang dat men aan de verschillende criteria toekent. Wanneer het van belang is dat de gebruiker geen actieve handeling verricht, valt vingerpatroonherkenning zeker af. Gezichtsherkenning scoort goed, maar de biometrische eigenschappen van het gelaat zijn minder gunstig. Wanneer de grootte van de apparatuur van minder belang is, scoort irisherkenning het hoogst.

Tabel 16 -Samenvatting beoordelingscriteria voor het toepassingsgebied 'look-alikes'

biometrie	weerstand tegen vandalisme	eigenschappen van het biometrisch kenmerk	betrouwbaarheid en 'proven technology'	geschiktheid eigenschappen en gebruik apparatuur
Gezichtsherkenning	n.v.t.		+	groot
Irisherkenning	n.v.t.	+	+	matig
Vingerpatroonherkenning	n.v.t.	+	+	gering
Stemherkenning	n.v.t.			gering
Dynamische handtekening	n.v.t.			zeer gering

Publieke kiosk - In tabel 17 is de samenvatting gegeven van de verschillende beoordelingen voor het toepassingsgebied publieke kiosk. Irisherkenning is de enige biometrische techniek die hier op alle beoordelingscriteria hoog scoort. Gezichtsherkenning scoort eveneens hoog, behalve m.b.t. de biometrische eigenschappen van het kenmerk.

Tabel 17 - Samenvatting beoordelingscriteria voor het toepassingsgebied publieke kiosk				
biometrie	**weerstand tegen vandalisme**	**eigenschappen van het biometrisch kenmerk**	**betrouwbaarheid en 'proven technology'**	**geschiktheid eigenschappen en gebruik apparatuur**
Gezichtsherkenning	+		+	zeer groot
Irisherkenning	+	+	+	zeer groot
Vingerpatroonherkenning	-	+	+	zeer gering
Stemherkenning	+			gering
Dynamische handtekening	-			zeer gering

Privé PC - In tabel 18 is de samenvatting gegeven van de verschillende beoordelingen voor het toepassingsgebied privé PC. Alleen vingerpatroonherkenning scoort voor dit toepassingsgebied op alle beoordelingscriteria positief. Gezichtsherkenning scoort goed, behalve wat betreft de biometrische eigenschappen van het kenmerk. De toepassing van irisherkenning is uitgesloten vanwege de hoge prijs.

Tabel 18 - Samenvatting beoordelingscriteria voor het toepassingsgebied Privé PC				
biometrie	**weerstand tegen vandalisme**	**eigenschappen van het biometrisch kenmerk**	**betrouwbaarheid en 'proven technology'**	**geschiktheid eigenschappen en gebruik apparatuur**
Gezichtsherkenning	n.v.t.		+	hoog
Irisherkenning	n.v.t.	+	+	zeer gering
Vingerpatroonherkenning	n.v.t.	+	+	voldoende/hoog
Stemherkenning	n.v.t.			voldoende/hoog
Dynamische handtekening	n.v.t.			matig/voldoende

Samenvatting en discussie - Nogmaals wordt er de nadruk opgelegd dat de eindresultaten van de beoordeling van de biometrische technieken zijn gebaseerd op een serie van achtereenvolgende beoordelingen. Bij ieder van deze beoordelingen heeft een zo zorgvuldig mogelijke weging plaatsgevonden van de biometrische technieken tegen de vastgestelde beoordelingscriteria. Het eindresultaat van al deze wegingen is echter schematisch en zal er mogelijk anders uitzien wanneer het belang van de verschillende parameters anders wordt gewogen dan hier is gebeurd.
In tabel 19 is de toepasbaarheid aangegeven van de verschillende biometrische technieken voor de verschillende toepassingsgebieden.

Tabel 19 - Toepasbaarheid biometrische technieken			
biometrie	**'look-alikes'**	**Publieke kiosk**	**privé PC**
Gezichtsherkenning	o	o	o
Irisherkenning	o	•	
Vingerpatroonherkenning			•
Stemherkenning			
Dynamische handtekening			

• positieve score op alle beoordelingscriteria

o positieve score op een belangrijk deel van de beoordelingscriteria

Gezichtsherkenning scoort positief voor alle toepassingsgebieden op de belangrijkste beoordelingsparameters. Het is echter van groot belang een eventuele toepassing van gezichtsherkenning te baseren op optimale, gestandaardiseerde omstandigheden van verlichting. Dit is echter niet praktisch realiseerbaar in het toepassingsgebied privé PC.
De apparatuur voor Irisherkenning heeft een ingebouwde standaardverlichting in het nabij infrarood.
M.b.t. vingerpatroonherkenning wordt opgemerkt dat deze voor het relevante toepassingsgebied zeer goedkoop moet zijn. Dit kan echter tengevolge hebben dat de kwaliteit van de biometrische apparatuur niet zeer hoog is. Met betrekking tot het toepassingsgebied privé PC zou daarom kunnen blijken dat het functioneren van de geselecteerde biometrische technieken minder gunstig zal uitpakken.

4.2.2 invloed van foutpercentages

In deze beoordeling zijn de foutpercentages van de verschillende biometrische technieken vooralsnog buiten beschouwing gelaten daar deze onderling niet zinvol vergelijkbaar zijn (§2.2.3). Wel zijn voor de verschillende toepassingsgebieden voorlopige eisen vastgesteld voor de FAR en de FRR (§2.2.2), deze zijn in tabel 20 nog eens samengevat.

Tabel 20 – Voorlopig vastgestelde toegestane foutpercentages			
type fout	**'look-alikes'**	**publieke kiosk**	**privé PC**
FRR	5%	0,5%	0,05%
FAR	0,1%	0,01%	0,001%
FTE	p.m.	p.m.	p.m.

Nu blijkt uit de praktijk dat, voor grote, zeer heterogene gebruikersgroepen, de percentages voor de FRR van biometrische technieken naar verwachting ruwweg tussen 1% en 5% zullen liggen (§2.2.3). Aannemend dat de voorlopig vastgestelde toegestane foutpercentages correct zijn, kan op grond daarvan allereerst worden geconcludeerd dat het gebruik van biometrie voor het toepassingsgebied privé PC waarschijnlijk niet eenvoudig kan worden gerealiseerd. Hierbij komt nog dat het functioneren van de voor dit toepassingsgebied geselecteerde biometrische technieken mogelijk minder gunstig zal zijn (§4.2.1).
De vereiste FRR voor toepassing van biometrie in een publieke kiosk ligt slechts weinig buiten de praktisch bereikbare percentages. Het is denkbaar dat een FRR van 0,5% kan worden bereikt bij toepassing van irisherkenning en zorgvuldige voorlichting. Gezichtsherkenning is een biometrische techniek die nog steeds wordt verbeterd en het verdient aanbeveling na te gaan in hoeverre een FRR van 0,5% voor deze techniek haalbaar is bij toepassing met grote heterogene gebruikersgroepen.

Daar iris- zowel als gezichtsherkenning passieve biometrische technieken zijn, en dus minder afhankelijk van de medewerking van de gebruiker, is het goed denkbaar dat de FTE gering zal zijn.
In hoeverre de vereiste waarden voor de FAR realiseerbaar zijn dient nader te worden onderzocht. Gezien de testresultaten van de pilot biometrie grenscontrole in Israël [8] (§2.2.3), waarbij de nagestreefde betrouwbaarheid van 0,1% voor de FRR en de FAR door geen van de 13 biometrische producten (6 verschillende biometrische technieken omvattend) werd gerealiseerd, lijkt dit niet voor de hand te liggen.

5 Conclusies

De in dit hoofdstuk verwoorde conclusies betreffen de selectie van biometrische technieken zowel a kritische succesfactoren voor het invoeren van biometrie op grote schaal.

Bij ieder van de beoordelingen heeft een zo zorgvuldig mogelijke weging plaatsgevonden van biometrische technieken tegen de vastgestelde beoordelingscriteria. Het eindresultaat van al deze weging is schematisch en zal er mogelijk anders uitzien wanneer het belang van de verschillende criteria ande wordt gewogen dan tijdens dit onderzoek is gebeurd. Dit resultaat kan daarom niet worden beoordee zonder de toelichtingen op de verschillende wegingen in aanmerking te nemen.

5.1 Selectie van biometrische technieken

1. Het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties verwacht dat alle reisdocument (paspoort en ID-kaart), met uitzondering van de nooddocumenten, in de toekomst zullen word voorzien van een mogelijkheid tot biometrische verificatie van de identiteit van de houder.

2. Het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties onderzoekt de mogelijkheid voor toepassing van biometrische technieken voor drie toepassingsgebieden: 'look-alikes', biometrisc kiosk in openbare ruimte en biometrie op een privé PC.

3. Het gebruik van biometrie in deze toepassingsgebieden zal zijn gebaseerd op de verificatieprocedu dat wil zeggen dat de controleprocedure de vraag dient te beantwoorden of de aanbieder van h reisdocument de rechtmatige houder daarvan is. Dit houdt in dat de biometrische template wor opgeslagen op het document zelf en niet in een centrale database.

4. De beschouwde toepassingsgebieden verschillen in de mate van begeleiding van de biometrisc controle en daarmee in het vereiste niveau van beveiliging.

Toepassing	Vorm	Vereiste niveau van beveiliging tegen fraude
'look-alikes'	Begeleid	laag
Kiosk in openbare ruimte	semi-begeleid	gemiddeld
PC in privé sfeer	niet begeleid	hoog

5. Op grond van de verschillen in het vereiste beveiligingsniveau tegen fraude tussen de verschillen toepassingsgebieden zijn voorlopige eisen aan de toegelaten foutpercentages false reject rate (FRR) false accept rate (FAR) gesteld.

Type fout	'look-alikes'	Publieke kiosk	privé PC
FRR	5%	0,5%	0,05%
FAR	0,1%	0.01%	0,001%

Deze eisen hebben overigens het doel de gedachten te richten en dienen niet beschouwd te worden a harde grenzen waaraan niet kan worden getornd.

7. De FRR van biometrische apparatuur - bij toepassing voor zeer grote, zeer heterogene gebruikersgroepen - wordt niet zozeer bepaald door de technische prestatie van de apparatuur zelf, maar eerder door het psychologische gebruikersprofiel. Tengevolge daarvan lijken de false reject cijfers van verschillende biometrische systemen elkaar in de harde praktijk niet bijzonder te ontlopen en zich in een gebied van ruwweg 1% tot 5% te bevinden. De FRR is hierom als middel tot het beoordelen van de bruikbaarheid van de verschillende biometrische technieken niet geschikt.

8. Over de FRR van verschillende biometrische technieken is te weinig bekend om op grond daarvan een keuze te kunnen maken voor een bepaalde biometrische techniek.

9. De vereiste FRR voor de toepassing van biometrie voor look-alikes ligt in de range van praktisch bereikbare percentages. Een succesvol gebruik van biometrie in dit toepassingsgebeid lijkt goed mogelijk.

10. De vereiste FRR voor toepassing van biometrie in een publieke kiosk ligt slechts weinig onder de praktisch bereikbare percentages. Een succesvol gebruik van biometrie in dit toepassingsgebied is mogelijk goed realiseerbaar.

11. Indien hetgeen is gesteld onder de conclusies 5 en 6 correct is, kan worden verwacht dat een succesvol gebruik van biometrie in het toepassingsgebied privé PC niet eenvoudig is te realiseren.

12. Op grond van de commerciële beschikbaarheid komen slechts de volgende vijf biometrische technieken voor nadere beschouwing in aanmerking (ten minste drie leveranciers):
    - gezichtsherkenning
    - irisherkenning
    - vingerpatroonherkenning
    - stemherkenning
    - herkenning van dynamische handtekening

12. Het beoordelingscriterium maatschappelijke acceptatie is uitgebreid besproken, het blijkt echter niet mogelijk om een zinvol onderscheid te maken tussen de verschillende biometrische technieken op basis van dit criterium. Omdat deze vermoedelijk als minder opdringerig zullen worden ervaren, zullen bij publieke toepassingen contactloze methoden naar verwachting beter scoren. dan methoden waarbij fysiek contact met de apparatuur moet worden gemaakt.

13. Een aantal biometrische technieken is geselecteerd die het beste kunnen worden ingezet voor de in dit onderzoek beschouwde toepassingsgebieden.

biometrie	**'look-alikes'**	**publieke kiosk**	**privé PC**
Gezichtsherkenning	o	o	o
Irisherkenning	o	•	
Vingerpatroonherkenning			•

• positieve score op alle beoordelingscriteria

o positieve score op een belangrijk deel van de beoordelingscriteria

Deze verdere selectie heeft plaatsgevonden op basis van de volgende beoordelingscriteria:

- weerstand tegen vandalisme
- eigenschappen van het biometrische kenmerk
- betrouwbaarheid en 'proven technology"
- eigenschappen en gebruik van biometrische apparatuur.

5.2 Kritische succesfactoren

In §3.1.5 is reeds ingegaan op de kritische succesfactoren van biometrische systemen, zoals deze door de verschillende geraadpleegde deskundigen naar voren werden gebracht. In het volgende zijn deze adviezen verder aangevuld.

Zeer grootschalige toepassingen van biometrie zijn in de afgelopen jaren gestart in Latijns Amerika en het Verre Oosten en geen enkele zeer grootschalige toepassing in Europa. Het invoeren van miljoenen gebruikers kan jaren duren en de mate van succes kan eerst worden beoordeeld wanneer deze toepassingen op de geplande volledige schaal functioneren. Zeer grootschalige, operationele toepassingen van biometrie voor zeer heterogene gebruikersgroepen bestaan momenteel nog niet, zodat kritische succesfactoren daaraan niet kunnen worden ontleend.

5.2.1 organisatie

1. Biometrie functioneert niet foutloos, daarom dient in adequate 'fall-back' procedures te zijn voorzien, waarbij zowel de functionaliteit voor de burger als het beoogde beveiligingsniveau moet worden gewaarborgd..

2. Een deugdelijke identificatie, vroeg in de keten van uitgifte van identiteitsdocumenten is noodzakelijk ten behoeve van een adequate introductie van elektronische identiteiten in Nederland.

3. De opslag van de biometrische data van de gebruikers in het systeem zowel als het daaropvolgende gebruik dienen onder een zorgvuldige begeleiding te geschieden. Hierbij dienen voorlichting en instructie als instrumenten te worden ingezet.

5.2.2 acceptatie door de gebruiker

1. De toepassing dient voor de gebruiker zinvol en nuttig zijn en als een duidelijke verbetering op de bestaande situatie te worden ervaren. De noodzakelijkheid dient door de gebruiker worden ingezien. Een goede communicatie naar de gebruiker is daarom van groot belang. Het moet de gebruiker volstrekt duidelijk zijn dat van de biometrische informatie geen misbruik kan of zal worden gemaakt.

2. Een hoge mate van gebruiksgemak dient te worden geboden, door ergonomische vormgeving en een omgeving waarin het gebruik eenvoudig en aantrekkelijk wordt gemaakt en additionele, externe druk wordt voorkomen.
   De biometrische apparatuur mag niet als opdringerig worden ervaren en dient, indien de gebruiker contact maakt met de apparatuur, eventuele hygiënische bezwaren te ondervangen. Het dient de gebruiker volstrekt duidelijk te zijn dat de biometrische apparatuur op geen enkele manier schade aan de gezondheid kan toebrengen.

De apparatuur dient een terugkoppelend signaal af te geven waardoor de gebruiker wordt geïnformeerd dat het biometrisch kenmerk op de juiste wijze wordt aangeboden.
Het vertrouwen van de potentiële gebruiker in de toepassing dient te worden gewekt door een degelijke uitstraling.

3. Het testen op het levend zijn van het aangeboden biometrische kenmerk kan de ervaring van betrouwbaarheid en daarmee de acceptatie bij de gebruiker doen toenemen.

4. De false reject rate dient zodanig laag te zijn dat de gemiddelde gebruiker geen onacceptabele last ondervindt van te frequente weigering van de gevraagde dienst t.g.v. het falen van de biometrische apparatuur.

5.2.3 betrouwbaarheid

1. De biometrische apparatuur dient voldoende foolproof te zijn. En storingsvrije werking is noodzakelijk, daar anders het risico bestaat dat de drempel door het bedienend personeel zal worden verlaagd teneinde de FRR te verlagen. Mogelijk kan een combinatie van biometrische kenmerken worden gebruikt om de betrouwbaarheid te vergroten.

2. De biometrische techniek dient bij voorkeur zo onafhankelijk mogelijk te zijn van fysieke variabelen als bloeddruk, manier van aanleggen, beschadiging, groei, littekens, enz. Ook de beschikbaarheid van het biometrische kenmerk dient voldoende te zijn: er moet altijd een alternatief zijn (zoals een andere vinger).

5.2.4 technologie

1. Biometrie is het meest betrouwbare middel voor persoonsauthenticatie. Niettemin vormt biometrie geen absolute oplossing, daar het gebruik ervan principieel gepaard gaat met een zeker foutpercentage (false rejects en false accepts).

2. Een combinatie met smart card en PKI (public key infrastructure) - in een verificatieketen – kan de betrouwbaarheid van biometrie mogelijk verhogen.

3. De apparatuur dient handzaam te zijn, met de mogelijkheid tot plug-and-play en integratie van hardware en software in bestaande platforms. Aandacht dient besteed te worden aan standaardisatie van de apparatuur.

4. De apparatuur dient ook goedkoop zijn, hoewel dit is een relatief gegeven is en een kosten-baten analyse hierin nader inzicht dient te geven.

6 Aanbevelingen

1. Het verdient aanbeveling de verschillende in dit rapport beschouwde toepassingsgebieden (look-alikes, publieke kiosk, privé PC) gedetailleerd te beschrijven en hiervoor een volledig programma van eisen op te stellen.

2. In dit rapport is een aantal beoordelingscriteria voor biometrische technieken voorgesteld. Op basis van een weging van deze criteria is een voorlopige selectie van biometrische technieken gemaakt. Het verdient aanbeveling een nader onderzoek in te stellen naar de voorgestelde criteria, de vereiste weging daarvan en de hieruit voortvloeiende selectie van biometrische technieken. In het bijzonder dient een nadere specificatie van de toegestane foutpercentages voor de verschillende in dit rapport besproken toegangsgebieden te worden opgesteld.

3. Het verdient aanbeveling de verschillende technische uitvoeringen van, uit de selectie resulterende, biometrische technieken nader te beschouwen op hun geschiktheid voor de verschillende in dit rapport beschouwde toepassingsgebieden. Eveneens dient te worden nagegaan in hoeverre nieuwe ontwikkelingen worden verwacht, en of deze, indien gewenst, probleemloos in het bestaande systeem kunnen worden ingevoerd. Hierbij dient mede te worden gelet op de mogelijke implementatie van API's (Application Program Interfaces) en de kosten-baten verhouding. Hiernaast is het denkbaar dat nu nog in ontwikkeling zijnde biometrische technieken volwassen worden en aan het criterium voor commerciële beschikbaarheid gaan voldoen.

4. Het verdient aanbeveling na te gaan in hoeverre een combinatie van biometrische kenmerken voordelen kan bieden voor de verschillende in dit rapport besproken toepassingsgebieden ("dual", of "layered authentication"). De vraag dient daarbij te worden beantwoord, welke kenmerken onder welke omstandigheden tezamen optimale resultaten geven. Het onderzoek dient ten minste de aspecten beveiliging, maatschappelijke acceptatie en juridische consequenties in aanmerking te nemen.

5. In deze studie is biometrie op zichzelf beschouwd. Het verdient aanbeveling na te gaan op welke wijze en in hoeverre de biometrische beveiliging tegen identiteitsfraude met een PKI (public key infrastructure) kan worden verhoogd. Hierbij wordt biometrie gecombineerd met een token (bijv. een smart card) en/of persoonlijke kennis (bijv. een wachtwoord) toegepast.

6. Op een groot aantal plaatsen ter wereld worden momenteel grootschalige civiele en sociale toepassingen van biometrie in gang gezet. Daar deze projecten in het beginstadium verkeren, zijn vooralsnog onvoldoende resultaten beschikbaar. Het verdient aanbeveling de ontwikkelingen op dit gebied, die als voorbeeld kunnen dienen voor de in dit rapport besproken toepassingsgebieden, nauwlettend te volgen.

Verwijzingen

[1] ANP bericht, vrijdag 27 Augustus 1999.
Kabinet wil elektronische pas naast paspoort
DEN HAAG (ANP) - Het kabinet wil naast het paspoort nog een identiteitskaart invoeren. Met de pas, waaraan een elektronische handtekening is gekoppeld, kan iedereen van achter de computer of telefonisch een uittreksel van het bevolkingsregister aanvragen, het rijbewijs verlengen, een uitkering regelen of mogelijk stemmen. Het plan staat in de begroting van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties, die volgende maand officieel verschijnt. Volgend jaar wordt het plan nader uitgewerkt. Met de nieuwe kaart, ter grootte van een bankpas, kan de houder zich op afstand identificeren door middel van een elektronische code. Ook is identificatie mogelijk door middel van unieke persoonsgegevens die op de kaart zijn opgeslagen, zoals vingerafdrukken.

[2] R. van Kralingen, C. Prins, en J. Grijpink, Het lichaam als sleutel - juridische beschouwingen over biometrie, ITER, Centrum voor Recht, Bestuur en Informatisering, http://www.nwo.nl/iter/publicaties.html

[3] Jan Grijpink, Identiteit als kernvraagstuk in een informatiesamenleving: een pleidooi voor een ketenbenadering, uitgave van het Ministerie van Justitie, 20 september 1998.

[4] *The Biometrics Report* (1995), Fingerprint, hand, eye, face, voice, signature; a research Report on Systems, Equipment, Costs, Advantages and Markets, by Emma Newham, ISBN 1 90018 00 9, 1995, 303 pages, Publ. S.J.B. Services, Somerset, UK - New York.

[5] Richards, D.R., "Rules of thumb for biometric systems", *Security Management*, October 1995, p. 67-71.

[6] Brad Wing, Overview of all INS biometric projects, CardTech/SecurTech '99, May 11-14, 1999, Chicago, USA, p. 543-552.

[7] Julian Ashbourn, The biometric white paper, (1999), www.biometric.freeserve.co.uk/whtpaper.htm.

[8] Arnon Harel, High security & high throughput for mass border crossing control system, CardTech/SecurTech '99, May 11-14, 1999, Chicago, USA, p. 411-421.

[9] James L. Wayman, Testing and evaluating biometric technologies, CardTech/SecurTech '98, April 27-30, 1998, Washinton, DC, USA, vol. 1, p 329-348, also downloadable from www.engr.sjsu.edu/biometrics as: Fundamentals of biometric technologies, U.S. National Biometric test Center, College of Engineering, San José State University, CA, USA.

[10] R.L. van Renesse, Selection of a biometric system, TNO-report, nr. HOI-RPT-970030, dd. 24 September 1997.

[11] R. Hes, T.F.M. Hooghiemstra en J.J. Borking, At face value, on biometrical identification and privacy, Achtergrondstudies en verkenningen, Registratiekamer, The Hague, september 1999.

[12] BioAPI Group, zie de website http://www.bioapi.org/ voor informatie.
Zie voorts:
B-API, Biometric API, http://www.iosoftware.com/bapi/index.htm
BioAPI, Biometric API Consortium, http://www.iosoftware.com/bapi/index.htm
HA-API, Human Authentication API, http://www.saflink.com/haapi.html

[13] Biometric Technology Today, vol.7, nr. 4, July/August 1999, p. 7.

[14] Richard Hopkins, Benchmarking very large scale biometric identity systems, Proceedings CTST '97, vol. 2, p. 313-332.

Appendix I - lijst van geïnterviewden

[redacted]
Enschedé/Sdu
Haarlem

[redacted]
Stichting NCP
Leidschendam

[redacted],
MINT
Gouda

[redacted]
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Den Haag

[redacted]
Ministerie van Justitie
Den Haag

[redacted]
Nedap - Security Control
Groenlo

[redacted]
Ministerie van Justitie, Immigratie en Naturalisatiedienst
Zwolle

[redacted]
Biometric Technology Today
Bankchambers, Langport
Somerset
UK

[redacted]
AND Identification
Rotterdam

[redacted]
Divisie Centrale Recherche Informatiedient
Zoetermeer

Appendix II - vragenlijst

Juridische aspecten

Welke juridische aspecten hangen samen met het toevoegen van een biometrische functie aan reisdocumenten?

Beveiliging

1. 'look-alike' problematiek

Voorzien wordt dat verificatie steeds zal plaats vinden onder toezicht van een ambtenaar. Sleutelen aan de apparatuur, aanbieden van imitaties, etc. maakt dan geen kans. Kan hierom gesteld worden dat het beveiligingsniveau van de biometrische verificatie niet hoog hoeft te zijn?

2. Elektronische identificatie op afstand

Hier zal nooit toezicht op de biometrische verificatie bestaan. Is het correct om aan te nemen dat de beveiliging daarom hoog dient te zijn? Welke factoren bepalen die beveiliging?

De foutpercentages (FAR en FRR) van biometrische apparatuur zijn zeer belangrijk. Maar in de praktijk lijkt weinig bekend te zijn over deze parameters. Is voor verschillende biometrische technieken globaal aan te geven hoe de praktijkcijfers liggen?

In hoeverre is een detectie van "leven en welzijn" van het biometrische kenmerk op biometrische apparatuur gerealiseerd en in hoeverre is deze detectie werkzaam? Is een dergelijke detectie voldoende om misleiding te voorkomen?

Toepasbaarheid en acceptatie

In hoeverre is er iets te zeggen over de "failure to enroll" van verschillende biometrische technieken?

Zijn u recente field tests bekend waarvan de rapportage verkrijgbaar is?

Is er iets in het algemeen te zeggen over de uniekheid van biometrische kenmerken? Bijvoorbeeld is de uniekheid alleen afhankelijk van het al of niet bestaan van erfelijke factoren of spelen er nog andere factoren een rol?

Is er iets te zeggen over de veroudering van biometrische kenmerken en de noodzaak tot een regelmatige update van de template?

Is er iets te zeggen over het discriminerend vermogen van biometrische apparatuur op lange termijn, d.w.z. de spreiding van de foutpercentages in de tijd?

Van welke biometrische technieken zou u zeggen dat ze in Nederland maatschappelijk aanvaardbaar zijn? Welke technieken zouden dit niet zijn?

Eigenschappen apparatuur

In hoeverre zijn er cijfers verkrijgbaar van de MTBF en de MTTR van biometrische apparatuur?

Wat is de huidige status van de ontwikkeling van biometrische APIs? Wanneer is te verwachten dat een generieke biometrische API gereed komt?

Welke biometrische technieken zijn goedkoop, welke zijn duur?

Welke technieken kunnen als "proven technology " worden beschouwd?

Grootschalige toepassingen

Welke zijn grootschalige toepassingen van biometrische technieken, die succesvol zijn? Waarom zijn ze succesvol?

Welke zijn grootschalige toepassingen van biometrische technieken, die niet succesvol zijn? En waarom zijn ze dat niet?

Wat zijn naar uw mening de kritische succesfactoren voor de gedachte biometrische toepassingsgebieden?

Appendix III – Foutpercentages

Recente informatie over biometrische foutpercentages (januari t/m november 1999)		
Bron	**Biometrie**	**Informatie**
Btt September 1999 vol.7, nr. 5	Vingerafdruk	Mytec Technology Gateway system: systems FTE rate is less than one percent, as is the accept/reject rate.
Btt May 1999 vol.7, nr. 2	Dynamische handtekening	Signature technologies have, on the whole, struggled to remove the final two percentage points in their error ratings.
Btt May 1999 vol.7, nr. 2	Stemherkenning	Domain Dynamics is now demonstrating speaker verification within the card chip. Lernout & Hauspie research indicates that their technology has an EER rate of 5% for a 336 byte template on an embedded chip, as against an EER of 3% for a larger template on a PC. This was taken for a single utterance of a public password. Using two passwords the testing showed 2% and 1% respectively.
Btt April 1999 vol.7, nr. 1	Vingerafdruk AFIS	Ultra-Scan test results. Model 805 software + (optical) Philippines data = FRR 5% at a FAR 0.05% (slightly poorer than the best performing AFIS vendor software, but within the workable design limits anticipated by the NBTC, of FRR 5% at FAR 0.1%. Model 805 software + (ultra sound) UltraScan data – FRR 0.5% at a FAR 0.04% < 0.06%. (Taken from graphs by UltraScan).
Btt March 1999 vol.6, nr. 10	Silicon finger sensors	Evaluation of fingerprint biometrics. After three month the trial has moved away from silicon sensors, having tried two of these without satisfaction. Dry fingers have also been a problem and the FTE rates are running at between five and ten percent. The move to optical technology is expected to solve some of these problems.
Btt March 1999 vol.6, nr. 10	Vingerafdruk	US National Biometric Test Center. The consortium already sees dual authentication with biometrics and smart cards as adequate insurance against relaxing FAR, although by keeping FRR at one percent or lower a real-world target is set for many fingerprint technologies.
Btt March 1999 vol.6, nr. 10	Handgeometrie	By adding another template to the verification matching calculation in Recognition System's (RSI) Handkey, the FRR in real world conditions can be reduced to 1.2%, claims [redacted] of Ukranian Bank Slavianskii.
Btt February 1999 vol.6, nr. 9	Gezichtsherkenning/ stemherkenning	Dual, or layered authentication: The current configuration layers face verification with speaker verification. HSI's [redacted] told Btt that, operating individually, the face and speaker verification modules have a FRR of about 6% when the FAR is close to zero. Joint operation reduces the false rejection rate to about 1%.
Btt February 1999 vol.6, nr. 9	Vingerafdruk AFIS	Based on the first 113,000 pairs of forefingers to be processed, [redacted] said that the FTE rate of the two-finger system was around 1.5%.
CardTech/SecurTech 1999 [8], Btt November 1999, vol. 7, nr. 7	Algemeen	Test biometrie bij dagelijkse grenscontrole op Palestijnse arbeiders in Israël: 11 leveranciers met 13 producten, die 6 verschillende biometrische technieken omvatten. Geen enkele getest product haalt nagestreefde betrouwbaarheid (FRR en FAR < 0,1%), slechts 2 producten (gezichtsherkenning en handgeometrie) voldoen aan de minimale betrouwbaarheidseisen (FRR incl. FTE < 3% en FAR <1%). Some solutions had FRRs up to 25% and many vendors did not know or had no clear idea of the FAR of their products before the trial began.
National Biometrics Test Center, San Jose, CA.	Vingerafdruk AFIS	Philippine Social Security System AFIS Benchmark Test Plan: It is the goal of this testing to assure that these search strategies do not drive the system non-match error rate over the allowable 5% level. http://www.engr.sjsu.edu/biometrics/publications_philippine.html
IND, Zwolle Vraaggesprek met [redacted] 13-09-1999.	Vingerafdruk	Vreemdelingenkaart. De FRR is circa 6%; de apparatuur blijkt zeer gevoelig voor hoek waaronder de duim wordt neergelegd. Veel hangt af van de begeleiding in het centrum tijdens enrollen en daarna. Ook als er een goede begeleiding is, schat [redacted] dat er een 2% tot 3% FRR zal bestaan.