Titel: Biometrische kenmerken: uniek maar niet geheim

Ter publicatie in het Handboek EDP-auditing december 2003.
Auteur: Dr. Eric R. Verheul
Senior Manager Global Risk Management Solutions
PricewaterhouseCoopers
eric.verheul@nl.pwc.com

Abstract
De meest gebruikte vorm van logische toegangsbeveiliging is gebaseerd op wachtwoorden, maar ook smartcards of andere hardware tokens worden vaak gebruikt. In dit artikel bespreken wij een derde en minder bekend type toegangsbeveiliging namelijk die gebaseerd op biometrische kenmerken, unieke kenmerken van wat een persoon *is* of *heeft* zoals een vingerafdruk. Het artikel geeft de lezer inzicht in de uitgangspunten, werking en terminologie van verschillende biometrische technieken en de daarop gebaseerde systemen voor toegangsbeveiliging. Verder worden de belangrijkste criteria voor biometrische systemen besproken en wordt op basis hiervan de bekendste negen biometrische systemen vergeleken, te weten: vingerafdruk, iris patroon, retina patroon, gezichtspatroon, infrarood gezichtspatroon, handtekening, stem, hand geometrie en hand bloedvaten patroon. Ook de potentiële zwakke plekken in biometrische systemen worden besproken. Dit stelt de lezer in staat een inschatting te maken van de situaties waarin biometrische authenticatie toepasbaar is, wat de meest geschikte systemen hierbij zijn en wat hierbij belangrijke aandachtspunten zijn.Tot slot bespreekt het artikel de belangrijkste normen rond biometrie en voorziet het de lezer van een aantal referenties voor verdere verdieping

Inhoudsopgave

1 Inleiding

In de Code voor Informatiebeveiliging ([F.]) wordt informatiebeveiliging beschreven als de instandhouding van de vertrouwelijkheid, integriteit en beschikbaarheid van informatie. Informatiebeveiliging wordt bereikt door de implementatie van verschillende typen maatregelen die organisatorische, personele, fysieke, juridische en ICT technische componenten kunnen hebben. Een belangrijk type maatregel daarbij is logische toegangsbeveiliging van informatiesystemen: een mechanisme dat zorgt draagt dat slechts geautoriseerde personen worden toegelaten, dat wil zeggen toegang kunnen krijgen tot bepaalde informatie of tot het kunnen uitvoeren van bepaalde transacties. Een impliciete eis bij logische toegangsbeveiliging is dat het mogelijk is met voldoende zekerheid vast te stellen *wie* een persoon is die wil worden toegelaten tot het informatie systeem. De gebruikelijke opzet daarbij bestaat uit twee onderdelen:

- Identificatie-claim, een persoon geeft aan wie hij is.
- Authenticatie, een persoon verstrekt voldoende zekerheid (‘bewijs’) dat hij deze persoon is.

De gebruikelijke toegangsbeveiliging bij informatiesystemen is gebaseerd op een identificatie-claim op basis van een userid en authenticatie op basis van het intypen van het wachtwoord behorende bij dit userid. Er bestaat een eenvoudige techniek, de zogenaamde ‘one time pad’ of Vernam cipher, die de vertrouwelijkheid van informatie op een ‘perfecte’ manier kan beschermen doordat de cryptografische sleutel éénmalig wordt gebruikt en net zo lang is als de boodschap. Er bestaat helaas echter niet zoiets als een ‘perfecte’ authenticatie techniek (en daarmee toegangsbeveiliging). De mate van zekerheid kan weliswaar zo groot worden gekozen als men belieft, maar de kans dat een oplichter er toch succesvol in slaagt zich voor een ander uit te geven is nooit nul. In de praktijk vormt dit echter geen probleem door deze kans voldoende klein te maken; hierbij dient het belang van de achterliggende informatiesystemen in ogenschouw te worden genomen. Voor wat betreft de authenticatie op basis van wachtwoorden vertaalt deze problematiek zich ondermeer tot de lengtekeuze van wachtwoorden.

In essentie zijn er slechts drie typen authenticatie van personen:

1. Kennis gebaseerd
   Dit is authenticatie op basis van ‘iets’ dat de persoon weet. Bekende voorbeelden zijn userids in combinatie met wachtwoorden of PIN codes.
2. Bezit gebaseerd
   Dit is authenticatie op basis van ‘iets’ dat de persoon in zijn bezit heeft. Bekende voorbeelden zijn bankpassen, smart cards en de ‘challenge-response’ tokens zoals in gebruik bij sommige electronic banking applicaties.
3. Biometrie gebaseerd (‘iets dat de persoon is’)
   Dit is authenticatie op basis van iets dat de persoon ‘is’, of preciezer op basis van specifieke, unieke fysiologische of gedragskenmerkende kenmerken die de persoon kan aantonen te hebben, *biometrische kenmerken* genaamd. Een bekend voorbeeld hiervan is authenticatie op basis van een vingerafdruk.

Dit artikel geeft een inleiding in het onderwerp biometrische authenticatie en stelt de lezer in staat een inschatting te maken in welke situaties dit type authenticatie

toepasbaar is, wat de meest geschikte systemen hierbij zijn en wat hierbij de aandachtspunten zijn. Het artikel is als volgt opgebouwd:

- Sectie 2 bevat de conclusie van dit artikel.
- Sectie 3 bespreekt het centrale uitgangspunt van biometrische authenticatie.
- Sectie 4 beschrijft de opzet van een generiek biometrisch systeem.
- Sectie 5 gaat in op de verschillende biometrische technieken die er bestaan.
- In Sectie 6 wordt een indicatieve vergelijking gemaakt tussen de verschillende biometrische systemen. Daartoe wordt eerst een algemene indeling gemaakt van de belangrijkste criteria voor biometrische systemen.
- Sectie 7, tenslotte, geeft een summier overzicht van de belangrijkste standaarden rond biometrische systemen.

De terminologie in de wereld van biometrie is niet altijd eenduidig; de in dit artikel gebruikte terminologie is zoveel mogelijk conform met de ANSI standaard X9.84-2001 “Biometric Information Management and Security”, indien we voor Engelse termen geen goed bruikbaar alternatief konden vinden, gebruiken we de Engelse term.

2 Conclusie

Biometrische kenmerken mogen principieel niet als geheime informatie worden beschouwd. Daarom is het van belang dat de partij die vertrouwt op de biometrische authenticatie voldoende zekerheid heeft dat alle componenten van een biometrisch systeem en de communicatie daartussen vrij van manipulatie zijn, hetgeen met fysieke (toezicht), technische (trusted devices) of cryptografische maatregelen (digitale handtekeningen) kan worden bereikt. Het gebruik van biometrie voor authenticatie op afstand, bijvoorbeeld over het Internet, stelt daarmee hoge technische eisen aan beveiliging.

Het is erg lastig om objectieve en volledige gegevens te krijgen over de accuraatheid van biometrische systemen en leveranciers van biometrische systemen spiegelen de prestaties van hun biometrische systemen vaak te mooi voor. Dit gebrek aan objectieve en volledige gegevens maakt het erg lastig voor organisaties om een goede haalbaarheidsanalyse uit te voeren inzake het gebruik van biometrie. Ons inziens vormt dit gebrek aan gegevens daarmee in feite een belemmering voor de acceptatie van biometrie in het algemeen. De realisatie van dergelijke gegevens zou ons inziens daarom een grote prioriteit moeten krijgen binnen de biometrische industrie. Leveranciers van biometrische systemen zijn er echter vaak nogal huiverig voor om (niet anoniem) vergeleken te worden met anderen en deze houding zal ons inziens moeten veranderen wil de biometrische markt echt volwassen worden.

De ANSI standaard X9.84 ([A.]) beveelt aan dat de kans dat een biometrische authenticatie een bedrieger niet afwijst $\leq 10^{-5}$ is. Hoewel deze eis voor biometrische systemen al moeilijk is te bereiken in de praktijk, komt deze kans vergeleken met authenticatie op basis userid/wachtwoord neer op het gebruik van wachtwoorden van hoogstens vier (kleine) letters uit het alfabet, terwijl bijvoorbeeld de Code voor Informatiebeveiliging ([F.]) minimaal zes karakters voorschrijft. Vanuit deze gedachte lijkt het gebruik van biometrische authenticatie als *enig* authenticatie middel voor de meeste informatiesystemen niet toereikend. Anders gezegd: biometrische authenticatie komt het beste tot zijn recht in combinatie met kennis (wachtwoord) of, en met name, bezit (smartcard) gebaseerde authenticatie.

Indien men biometrische authenticatie wil gebruiken conform de genoemde ANSI X9.84 aanbeveling dan komt men uit op het gebruik van één de volgende biometrische kenmerken: vingerafdrukken, iris patronen, retina patronen of een combinatie van minder accurate biometrische technieken (multi-factor biometrie). Bij biometrische systemen gebaseerd op vingerafdrukken is een aandachtspunt dat deze gevoelig zijn voor misleiding van de sensor (‘gummy fingers’). Het gebruik van retina patronen kan op weerstand stuiten omdat bij het bepalen het oog van de gebruiker dicht (6-8 cm) bij de sensor dient te houden en ook omdat hierbij gebruik wordt gemaakt van zwak laserlicht waar gebruikers veelal huiverig voor zijn. Retina sensors zijn daarbij relatief duur. Tot slot kleven er aan zowel het gebruik van het iris als retina patroon potentiële privacy issues omdat zij als bijzondere persoonsgegevens kunnen worden gezien daar zij dicht tegen medische gegevens aanzitten. Inzake het iris patroon bestaat zelfs een (pseudo-)wetenschap, irisscopie, die pretendeert uit het iris patroon iemands gezondheid te kunnen aflezen.

3 Het uitgangspunt van biometrische authenticatie

Zoals we al gesteld hebben in de inleiding is biometrische authenticatie gebaseerd op specifieke, unieke fysiologische of gedragskenmerkende kenmerken die de persoon kan aantonen te hebben. De zinsnede ‘aantonen te hebben’ hierin, dat wil zeggen een bepaalde actieve of passieve ‘vaardigheid’ (‘ability’ in het Engels) van de persoon, is het karakteristieke aspect van biometrische authenticatie. Het cruciale (ideale) uitgangspunt van de biometrie is dat deze specifieke *vaardigheid* niet overdraagbaar dient te zijn aan anderen zelfs met de medewerking van de persoon in kwestie. In het bijzonder impliceert dit dat een **vastlegging** van het feitelijke kenmerk (bijvoorbeeld een vingerafdruk) een aanvaller niet kan helpen om deze vaardigheid te verkrijgen. Kernachtig geformuleerd: biometrische authenticatie is gebaseerd op een unieke vaardigheid zonder geheimen. Dit uitgangspunt is zeer belangrijk omdat dit betekent dat gebruikers van biometrische systemen hun kenmerken niet geheim hoeven te houden of dat ze zich zorgen hoeven te maken dat een eenmaal verstrekt biometrische kenmerk aan een partij A, later door die partij kan worden misbruikt om toegang te krijgen bij partij B die dit biometrische kenmerk ook gebruikt voor authenticatie. Vooruitlopend op Sectie 6.1 kunnen er overigens wel privacy redenen zijn om een biometrische kenmerk geheim te houden maar dat is een andere kwestie.

Absolute zekerheid dat biometrische kenmerken bestaan die voldoen aan het uitgangspunt zal waarschijnlijk nooit kunnen worden gegeven, dergelijke zekerheid kan hoogstens empirisch van aard zijn. Maar zelfs als dergelijke kenmerken bestaan dan valt of staat de kwaliteit van de biometrische systemen, die we zullen beschrijven in de volgende sectie, nog met de (geautomatiseerde) wijze waarop met deze kenmerken wordt omgesprongen.

4 De opzet van een biometrisch systeem

In Sectie 4.1 zullen wij de componenten van een generiek biometrisch systeem bespreken. Door deze componenten op de voor de handliggende wijze in te vullen ontstaat de opzet zoals die vaak wordt gebruikt bij fysieke toegangsbeveiliging. In Secties 4.2, 4.3 zullen we twee andere invullingen bespreken die nauw samenhangen met Public Key Infrastructures (PKIs): het gebruik van biometrie voor smartcard toegangsbeveiliging en het gebruik van digitale certificaten voor de opslag van biometrische gegevens.

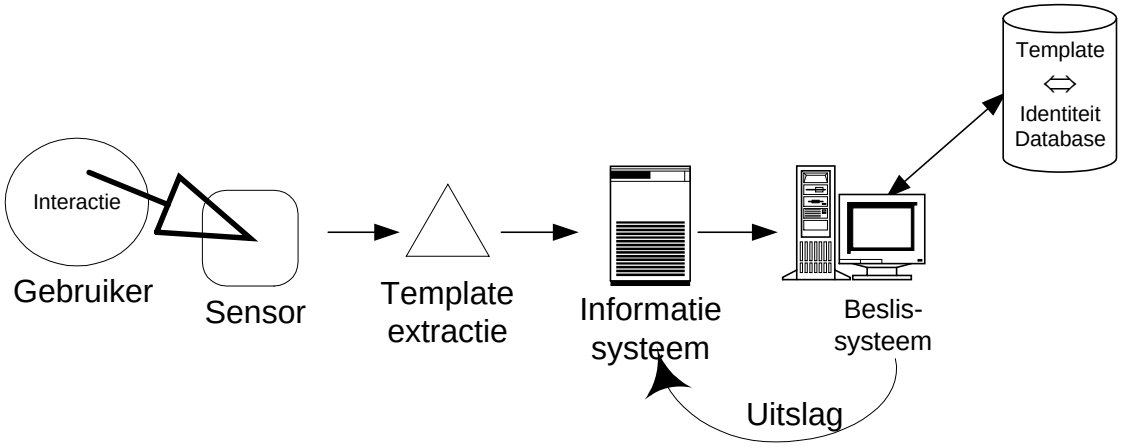
4.1 Generieke opzet

In opzet bestaat een generiek biometrisch systeem uit de volgende onderdelen (zie ook onderstaand diagram):

- Een gebruiker wil toegang tot een bepaalde informatiesysteem en heeft daartoe een interactie met een *sensor* van het biometrisch systeem waarmee het biometrisch kenmerk bepaald kan worden. (bijvoorbeeld, legt zijn vinger op een vingerafdruk lezer).
- De sensor levert een signaal naar hardware/firmware/software dat hieruit op basis van een bepaald algoritme een digitale representatie, *biometrisch template* genoemd, extraheert. Dit template wordt, al dan niet via het informatiesysteem waar de gebruiker toegang toe probeert te krijgen, doorgestuurd naar het biometrische beslissysteem.
- Het biometrisch beslissysteem beheert de templates en de gerelateerde meta-informatie zoals identiteiten en neemt op basis van een bepaalde heuristiek beslissingen over het wel of niet voorkomen van het kenmerk in de database en deze beslissingen terugkoppelt naar het informatiesysteem.

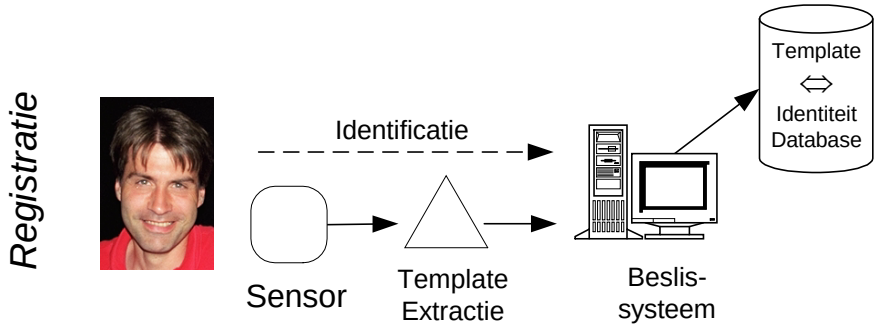
Biometrische extractie en beslis algoritmen worden vaak niet geopenbaard door de leverancier, dat wil zeggen zijn ‘proprietary’.

In een perfect biometrisch systeem zou het biometrisch template bij verschillende bepalingen steeds hetzelfde zijn en hebben alle personen een uniek biometrisch template. Op basis van een vastgelegde koppeling tussen de identiteit van personen en hun biometrische kenmerken kan dan op evidente wijze authenticatie plaatsvinden. Helaas bestaan er geen perfecte biometrische systemen en zullen de biometrische templates van dezelfde persoon afkomstig van verschillende bepalingen weliswaar op elkaar lijken maar toch vaak verschillend zijn. Dit kan het gevolg zijn van verschillende omstandigheden, zoals bijvoorbeeld een andere plaatsing van een vinger op een vingerafdruk lezer. Ook zullen de biometrische templates van verschillende personen meestal voldoende verschillend zijn maar niet altijd. Om deze redenen beschikt een biometrisch systeem altijd over een beslissysteem gebaseerd op een bepaalde heuristiek; hier komen we direct op terug.

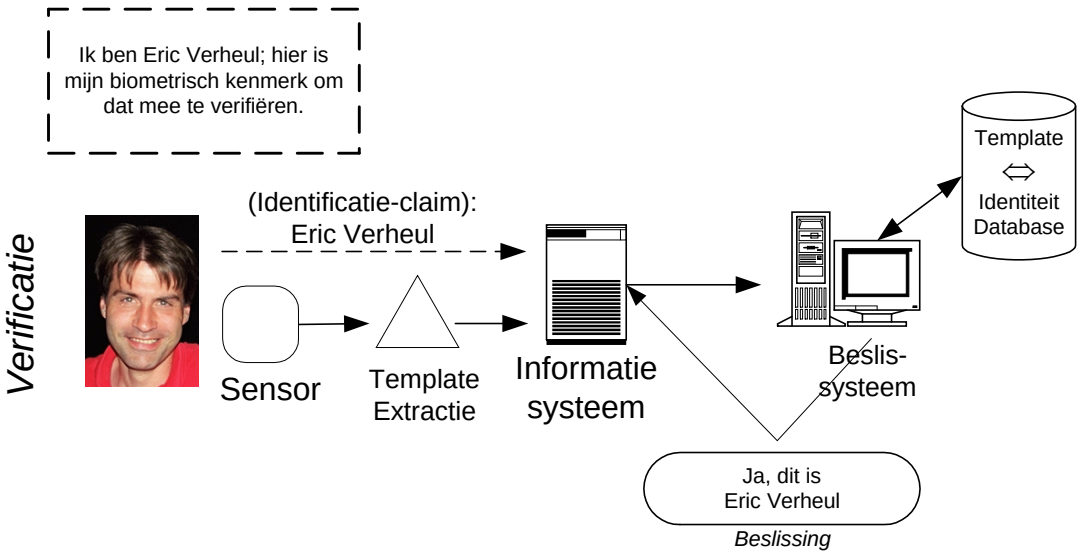


Er bestaan drie belangrijke processen rond een biometrisch systeem:

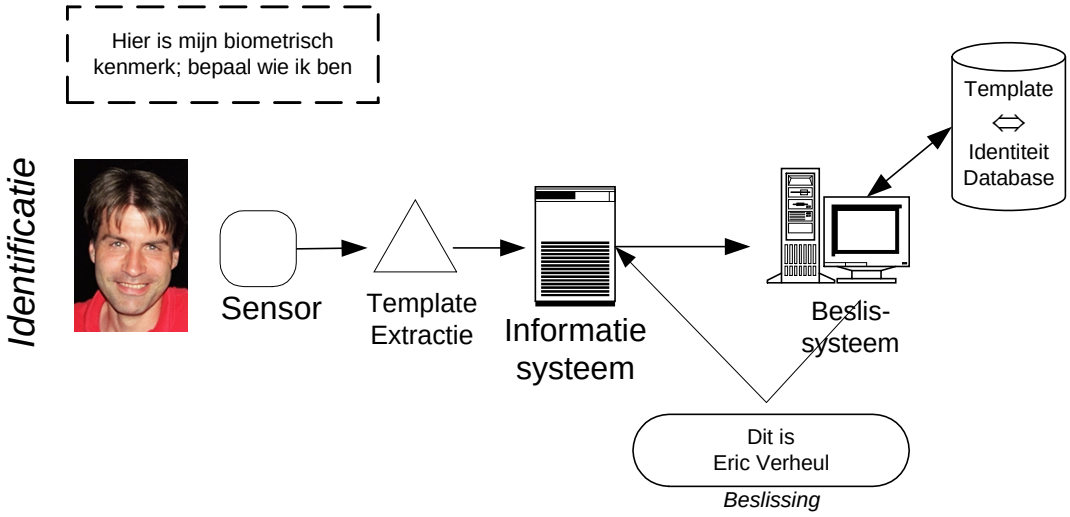
1. Vastlegging en registratie van biometrisch kenmerk (‘Enrollment’)
   Hierbij wordt een biometrisch template van een persoon bepaald en wordt dit gekoppeld aan diens identiteit en geplaatst in de centrale database van het systeem. Om een biometrisch template van goede kwaliteit te verkrijgen, worden vaak meerdere bepalingen uitgevoerd. De kwaliteit van deze koppeling is één van de bepalende factoren voor de kwaliteit van het gehele systeem. Een hoge kwaliteit van deze koppeling kan bijvoorbeeld bereikt worden door de gebruikers te verplichten in persoon naar een registratie locatie te komen en na bepaling van zijn biometrische template de gebruiker zich te laten authenticeren met een hoogwaardig identiteitsbewijs zoals een nationaal identiteitsbewijs.



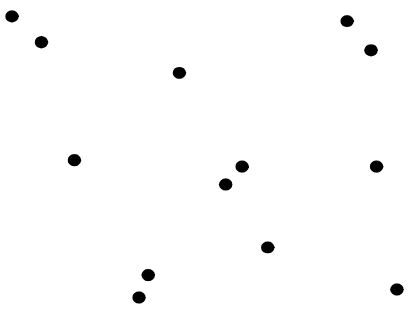
2. Gebruik van een biometrisch kenmerk
   a) Verificatie (‘one-to-many comparison’, ‘closed search’)
   Bij dit gebruik wordt een persoon gevraagd om zijn identiteit (bijvoorbeeld zijn naam) en om zijn biometrisch kenmerk te laten bepalen. Het beslissing systeem beoordeelt of daaruit geëxtraheerde biometrische template ‘voldoende’ lijkt op het template zoals dat in de centrale database opgeslagen is voor deze identiteit. Indien dit het geval is, is de persoon geverifieerd en anders wordt hij als niet-geverifieerd bestempeld. Net zoals bij userid/wachtwoord gebaseerde authenticatie is het mogelijk om bij herhaalde, bijvoorbeeld drie, onsuccesvolle verificaties het gerelateerde account te blokkeren.



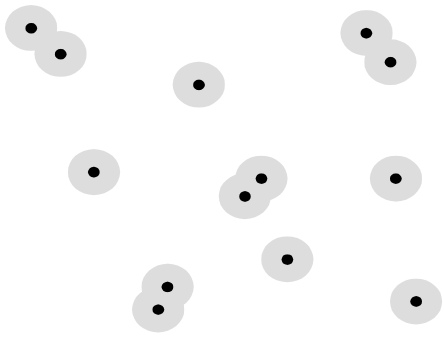
b) Identificatie (‘one-to-many comparison’, ‘open search’)
Bij dit gebruik wordt een persoon slechts gevraagd om zijn biometrisch kenmerk te laten bepalen. Het beslissing systeem beoordeelt welk opgeslagen biometrisch template ‘voldoende’ lijkt op het bepaalde biometrische template. Indien er sprake is van een voldoende betrouwbare oplossing dan wordt de persoon daarmee geïdentificeerd anders wordt de persoon als niet-geïdentificeerd bestempeld. In essentie is identificatie moeilijker dan verificatie en stelt veel hogere eisen aan de kwaliteit van een biometrisch systeem, met name als er veel gebruikers geregistreerd zijn. We merken verder op dat de betekenis van de term identificatie in de biometrie anders is dan de betekenis in de algemene context van informatiebeveiliging.



De kwaliteit van de verificatie en identificatie van een biometrisch systeem is in hoge mate afhankelijk van de mate waarin later bepaalde biometrische templates van een persoon mogen verschillen van het template zoals bepaald tijdens de registratie. Deze mate van verschil wordt binnen een biometrisch systeem ingesteld aan de hand van een drempelwaarde: een later bepaald template dat minder dan de drempelwaarde afwijkt van een geregistreerd template wordt daarmee geassocieerd. Om dit verder te verduidelijken zullen we alle biometrische templates van een persoon bij een bepaald systeem **binnen** een ingestelde drempelwaarde visualiseren als een bol in het platte vlak rond het geregistreerde template; een hogere drempelwaarde zou in grotere bollen resulteren. Vergelijk onderstaande figuur.



Biometrische templates: ideaal



Biometrische templates: praktijk

De uitdaging is nu om te zorgen dat enerzijds deze systeembollen geen overlappingen hebben en anderzijds dat de gemeten templates van personen in de praktijk binnen hun voorgeschreven systeembollen vallen. Aan deze uitdaging zijn twee maten voor de accuraatheid van een biometrisch systeem verbonden:

- False Non-Match Rate (FNMR)
  De kans dat een biometrisch systeem een verificatie van de identiteit van een legitieme gebruiker onjuist uitvoert (ook wel 'false negative' genoemd). In andere woorden: een legitieme gebruiker A claimt dat zijn identiteit A is maar wordt (onterecht) afgewezen op basis van zijn biometrisch kenmerk. In de visualisatie van de bollen betekent dit dat het gemeten biometrisch kenmerk van persoon A buiten diens systeembol terecht is gekomen. In zijn algemeenheid geeft kleinere systeembollen een grotere kans op een False Non-Match. De waarde FNMR is ook bekend als False Rejection Rate (FRR).
- False Match Rate (FMR)
  Hoewel dit enigszins verwarrend is, bestaan er twee versies van de False Match Rate:
    - False Match Rate of Verification (FMRV)
      De kans dat een biometrisch systeem een persoon onjuist **verifieert**. In andere woorden: de kans dat een bedrieger die claimt dat hij persoon A is, niet afgewezen wordt door het biometrische systeem.
    - False Match Rate of Identification (FMRI)
      De kans dat een biometrisch systeem een persoon onjuist **identificeert**. In andere woorden: de kans dat een (mogelijk geregistreerde) gebruiker door het biometrische systeem onterecht wordt aangemerkt als een (ander) geregistreerd persoon.

  In de visualisatie van de cirkels betekenen beide onjuiste gebeurtenissen dat het gemeten biometrische kenmerk van de bedrieger/gebruiker in de systeembol van persoon A terecht is gekomen. In zijn algemeenheid geeft grotere systeembollen een grotere kans op een False Match. We merken nog op dat False Matches ook wel 'false positives' worden genoemd en dat de term FMR ook bekend staat als False Acception Rate (FAR).

De definitie die de ANSI X9.84 standaard ([A.], zie ook Sectie 7), gebruikt voor de FMR waarde is ons inziens een merkwaardige combinatie van de FMRV en FMRI waarde, we citeren: [False Match Rate is] *the probability that a biometric system will incorrectly identify an individual, or fail to reject an imposter*. Behalve dat ons inziens onduidelijk hoe deze waarde überhaupt eenduidig te bepalen is, is de ANSI definitie van de FMR waarde ons inziens ook weinig praktisch relevant omdat men veelal in de praktijk een bepaald biometrisch systeem gebruikt wordt voor verificatie *of* identificatie maar niet voor allebei tegelijkertijd; voor de eerste toepassing is de FMRV waarde relevant voor de tweede de FMRI waarde.

De eerste interpretatie van het begrip FMR is de gangbare (vergelijk ook [G.]) en die interpretatie (en notatie) zullen wij dan ook aanhouden in dit artikel. Men kan beargumenteren dat heel grofweg het volgende verband bestaat tussen de FMRI en FMRV waarden:

$$\text{FMRI} \approx \text{FMRV} \times \#(\text{Gebruikers van het biometrisch systeem}).$$

Immers, de FMRV waarde is de kans dat een willekeurig individu in een specifieke systeembol terecht komt en de FMRI waarde is de kans dat een willekeurig individu in een willekeurige systeembol terecht komt. Hiervan zijn er net zoveel zijn als er geregistreerde gebruikers binnen het biometrisch systeem zijn. Uitgaande van niet overlappende systeembollen komt men dan tot bovenstaande formule. Uit deze formule spreekt duidelijk dat:

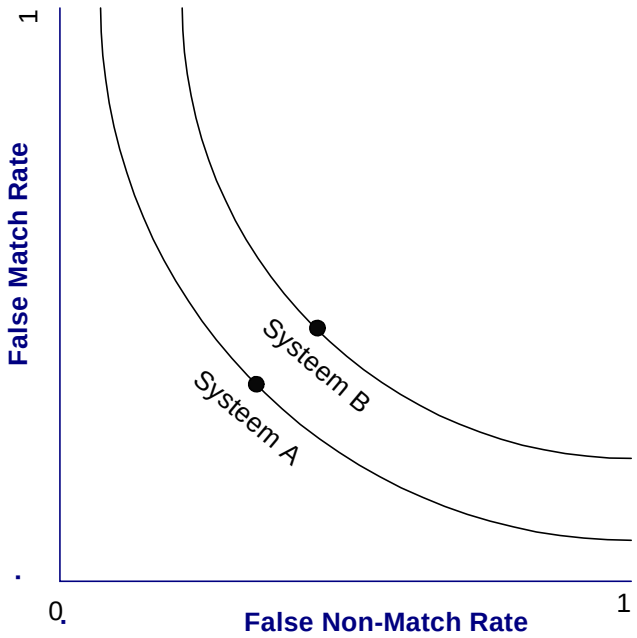
- de FMRI waarde groter is dan de FMRV waarde,
- dat identificatie dus moeilijker is dan verificatie en ook steeds (min of meer lineair) moeilijker wordt met het aantal gebruikers in het systeem.

Al met al betekent dit dat slechts systemen met een erg lage FMRV waarde kunnen worden gebruikt voor identificatie.

In zijn algemeenheid is het streven naar een biometrisch systeem dat zowel een kleine False Non-Match Rate als een kleine False Match Rate heeft, maar helaas zijn beide maten zijn sterk aan elkaar gerelateerd zij het omgekeerd:

- Een kleine FNMR betekent grote systeembollen en dus een grote FMR.
- Een kleine FMR betekent kleine systeembollen en dus een grote FNMR.

De bandbreedten van beide maten zijn sterk afhankelijk van het type biometrisch systeem maar hun onderlinge verhouding is in zekere mate configureerbaar binnen elk biometrisch systeem. Het is dus mogelijk om een FMR waarde te hebben van bijna 0, maar de FNMR waarde zal dan bijna 1 zijn. Vergelijk onderstaande illustratieve grafiek waarin de relatie tussen FMR en FNMR is geïllustreerd voor twee biometrische systemen A en B. Hierbij is systeem A technisch beter dan B. A zou bijvoorbeeld kunnen corresponderen met vingerafdrukken en B met gezichtsherkenning. Een FMR waarde van systeem zonder FNMR waarde zegt daarom theoretisch gezien weinig.



Het belang van het informatiesysteem waarmee via biometrische authenticatie toegang tot kan worden verkregen zal eisen stellen aan daarmee gehanteerde waarden van FNMR en FMR en hun verhouding. Hierbij zal de eis aan de FMR waarde (‘de kans dat er ongeautoriseerde transacties kunnen worden uitgevoerd’) rechtstreeks

verband houden met de waarde van de transacties die daarmee kunnen worden uitgevoerd. De eisen rond de FNMR waarde (‘de kans dat er geen geautoriseerde transacties plaats kunnen vinden’) zullen samenhangen met de benodigde beschikbaarheid van het informatie systeem. Bij een financieel transactie systeem zal een lage FMR waarde veelal belangrijker zijn dan een lage FNMR waarde, bij een alarmeringsysteem waar het zekere voor het onzekere wordt genomen, zal het eerder andersom zijn.

Soms worden de FNMR en FMR gelijk gekozen, ook wel de Equal Error Rate (EER) genoemd, aangegeven in bovenstaande figuur als punten. De EER is een goede maat voor de technische kwaliteit van een biometrisch systeem; hoe kleiner de EER hoe beter de kwaliteit.

De (financiële) ANSI standaard X9.84 (zie [A.]), stelt dat beide typen FMR waarde (FMRV en FMRI) minimaal kleiner of gelijk moeten zijn op de kans dat een vier-cijferige PIN code wordt geraden oftewel 10^{-4}. De standaard beveelt echter $\leq 10^{-5}$ aan. De ANSI standaard stelt geen kwantitatieve eisen aan de FNMR waarde. In [C.] wordt aanbevolen dat de FNMR waarde $\leq 10^{-2}$ is.

Hoewel een FMR waarde van 10^{-5} in de praktijk al moeilijk te halen is voor biometrische systemen, is deze waarde vergeleken met userid/wachtwoord authenticatie erg ongunstig hoog. Om dit toe te lichten: de Code voor Informatiebeveiliging ([F.]) stelt zes als minimale lengte eis voor wachtwoorden. De complexiteit van een wachtwoord hangt behalve van diens lengte ook af van de karakterset waaruit deze gekozen wordt. Als we uitgaan van de eenvoudigste karakterset namelijk het alfabet zonder hoofdletter, dat wil zeggen bestaande uit 26 karakters, dan is een kans van 10^{-5} groter dan de kans van het raden van een dergelijk wachtwoord van lengte kleiner ≤ 4, immers $1/(26^4+26^3+26^2+26) = 1/475.254 \approx 2 . 10^{-6} < 10^{-5}$. Vanuit dit simpele rekensommetje lijkt het gebruik van biometrische authenticatie als enig authenticatie middel voor de meeste informatiesystemen niet toereikend. Anders gezegd: biometrische authenticatie komt het beste tot zijn recht in combinatie met kennis (wachtwoord) of, en met name, bezit (smartcard) gebaseerde authenticatie.

4.2 Biometrische toegangsbeveiliging tot smartcards

Onder een smartcard wordt over het algemeen een Intergrated Circuit (‘chip’) verstaan met een processor, RAM geheugen en een soort kleine harde schijf ((E)EPROM). Op smartcards bevinden zich vaak cryptografische sleutels waarmee de smartcard of diens eigenaar zich bijvoorbeeld kan authenticeren bij informatiesystemen. Een actueel voorbeeld van dergelijke smartcards zijn Public Key Infrastructure (PKI) smartcards waarmee de eigenaar in staat is om een digitale handtekening te plaatsen op een digitaal document. Dergelijke handtekeningen zijn gebaseerd op public key cryptografie waarbij de private sleutel gebruikt wordt door de eigenaar voor het plaatsen voor de handtekening en de publieke sleutel voor de controle daarvan door anderen. Daartoe wordt de publieke sleutel samen met identificerende gegevens van de gebruiker digitaal ondertekend door een Certification Authority, resulterend in een digitaal certificaat. In de Verenigde Staten en in de cryptografie wordt overigens gesproken over een digitale handtekening en binnen de Europese instellingen over een elektronische handtekening hetgeen een iets ruimer

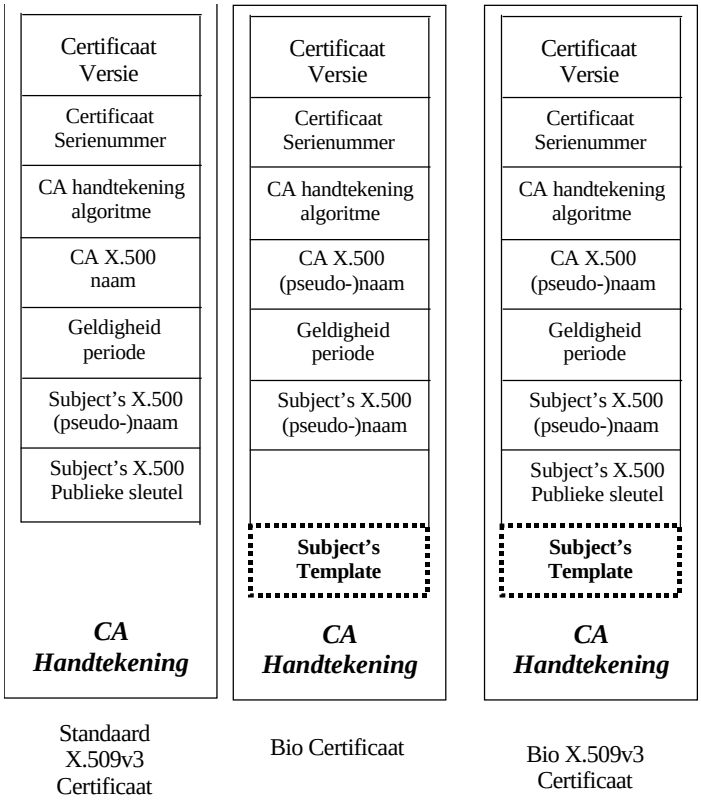
begrip is. Er bestaat een Europese richtlijn (1999/93/EG) die onder bepaalde voorwaarden digitale handtekeningen juridisch gelijk stelt aan conventionele (handgeschreven) handtekeningen. Deze voorwaarden betreffen ondermeer de kwaliteit van het certificaat uitgifte proces en de bescherming van de private sleutel op de smartcard (in dit verband Secure Signature Creation Device of SSCD genoemd) tegen onbevoegd gebruik. Veelal wordt het gebruik van de private sleutel beschermd met een PIN code, maar een alternatief of aanvulling kan het gebruik van biometrie zijn. Hierbij kan de PC van de gebruiker bijvoorbeeld zowel verbonden zijn met een smartcard lezer als met een vingerafdruk sensor en kan de gebruiker pas een handtekening op een document zetten indien deze zich succesvol heeft geauthenticeerd met zijn vingerafdruk. Op 21 mei 2003 is de Wet elektronische handtekeningen in werking getreden die de Europese richtlijn implementeert.

4.3 Bio certificaten

Digitale certificaten in de gebruikelijke vorm leggen een verband tussen een publieke sleutel en de identiteit of pseudoniem van de eigenaar. Een certificaat kan ook anoniem zijn hetgeen we gemakshalve beschouwen als een pseudoniem certificaat waarbij het gekozen pseudoniem de ‘lege string’ is. De belangrijkste standaard op dit terrein is X.509 versie 3 (ISO/IEC 9594-8), zie het linker certificaat in onderstaand figuur. Behalve dat biometrische technieken gebruikt kunnen worden om de toegangsbeveiliging tot private sleutels af te schermen (zie Sectie 4.2) zijn er ook ontwikkelingen om biometrische informatie op te nemen als onderdeel (‘extensie’) van een digitaal X.509 certificaat. In de Verenigde Staten is bijvoorbeeld het National Security Agency (NSA) met deze ontwikkeling bezig vanuit het Tokeneer project (zie [J.]). Maar ook op eigen bodem (Enschedé/Sdu) is men bezig met de ontwikkeling van deze opzet.

Het opnemen van biometrische informatie in digitale certificaten kan op diverse wijzen, waarvan wij er twee bespreken:

- Het toevoegen van een biometrisch template van de eigenaar aan een X.509v3 extensie veld aan een X.509v3 certificaat (‘Bio X.509v3 certificaat’) zodat niet alleen alle standaard X.509 informatie digitaal wordt ondertekend door de Certification Authority maar ook het biometrische template van de eigenaar. Zie het rechter certificaat in onderstaand figuur.
- Het zelfde type certificaat waarbij de publieke sleutel informatie van de eigenaar niet is toegevoegd (‘Bio Certificaat’). Zie het certificaat in het midden van onderstaand figuur. In feite is dit type certificaat dan geen publieke sleutel certificaat meer.



Het voordeel van een Bio Certificaat is dat dit decentrale biometrische authenticatie mogelijk maakt zonder dat er een on-line verbinding hoeft te bestaan tussen het beslissysteem en een centrale database met alle geregistreerde templates daarin. Immers, de gebruiker biedt zijn Bio Certificaat aan (vanaf een floppy of een smartcard), het biometrie station verifieert de CA handtekening daarop en kijkt of het certificaat niet ingetrokken is (CRL check). Indien dit succesvol is, vraagt het station de gebruiker om diens biometrische kenmerk te laten bepalen, hetgeen vervolgens wordt vergeleken met het template opgeslagen in het certificaat. Indien deze stap ook succesvol is, kan het station de autorisatie van de gebruiker op basis van diens (pseudo-)naam bepalen dat ook in het certificaat is opgeslagen.

Daar Bio X.509v3 certificaten additioneel de gebruikelijke mogelijkheden van een standaard X.509v3 certificaat hebben, kan er ook een challenge-response protocol op worden gebaseerd waarmee de eigenaar van het certificaat kan bewijzen dat hij beschikt over de (geheime) private sleutel behorende bij de publieke sleutel in het certificaat. Met andere woorden Bio X.509v3 certificaten maken twee factor authenticatie mogelijk. Indien deze private sleutel zich op een trusted device (zoals een smartcard) bevindt, is zelfs drie factor authenticatie mogelijk.

Een belangrijk aandachtspunt bij het plaatsen van biometrische data in certificaten is privacy, daar certificaten veelal als publieke informatie worden gebruikt. Vergelijk Sectie 6.1. Binnen deze opzet kan de biometrische data daarom het beste versleuteld worden zodat slechts beperkte partijen (bij voorkeur ter beslissing van de gebruiker) over deze data kunnen beschikken, dit maakt deze opzet wel complexer.

5 De verschillende biometrische kenmerken

In deze sectie bespreken we de bekendste biometrische kenmerken en zullen deze toetsen tegen enkele intuïtief duidelijke criteria. Deze criteria en de toetsing van de besproken technieken zullen we nader uitwerken in Sectie 7.

5.1 Vingerafdruk

De binnenkant van onze handen, vingers en de onderkant van onze voeten en tenen hebben van dichtbij een 'corduroy'-achtig patroon gevormd door zogenaamde frictieplooien. Deze plooien kunnen allerlei karakteristieken hebben, *minutiae* genaamd. Zo zijn er plooien die een vork vorm hebben of die een gesloten kromme vormen ('eiland'). Het idee is dat een voldoende aantal van deze *minutiae* en hun onderlinge positie op een bepaalde vinger een betrouwbaar onderscheidend kenmerk van een persoon is; zelfs eeneiige tweelingen kunnen hiermee onderscheiden worden. Vingerafdrukken worden gevormd tijdens het foetale stadium en blijven daarna ongewijzigd. Vingerafdrukken zijn zeer goed in staat om personen te onderscheiden en worden daarom al meer dan een eeuw gebruikt als bewijsmateriaal tijdens rechtszittingen. Op http://bias.csr.unibo.it/fvc2002 wordt een evaluatie gegeven van een aantal biometrische systemen gebaseerd op vingerafdrukken, waarbij helaas een flink aantal leveranciers verkozen anoniem te blijven.

Het bepalen van een vingerafdruk vindt soms plaats met een optische (CCD) camera maar meestal met een 'capacitieve' sensor. Laatst genoemde sensors meten spanningsverschillen verschillen tussen een fors aantal meetpunten op een vingertop. Door de geringe omvang van een vingerafdruk en sensor is het mogelijk om de sensor te integreren in standaard randapparatuur zoals een muis (BioMouse) of een toetsenbord (Secure Keyboard Scanner). Het bepalen van een vingerafdruk wordt niet als belastend ervaren door gebruikers. Hierbij is wel enige training/uitleg nodig is voor gebruikers omdat de juiste plaatsing van de vinger op de sensor van belang is. Invloeden als beroep (bijvoorbeeld vieze, droge of extreem gladde vingers), leeftijd of specifieke omstandigheden (verlies of verwondingen van vingers) kunnen betekenen dat de vingerafdrukken van een persoon niet bruikbaar zijn als biometrisch kenmerk. Hoewel het hier slechts een kleine fractie van de wereld populatie betreft dient bij het overwegen van vingerafdruk biometrie de doelgroep op dit punt wel te worden beoordeeld. Met het tijdelijk niet beschikbaar zijn van een vinger door bijvoorbeeld een verwonding kan rekening worden houden door altijd twee vingers van twee verschillende handen in te scannen en identificatie of verificatie mogelijk te maken op elk van deze vingers. Biometrische systemen op basis van vingerafdrukken kunnen een erg lage FMR waarde (orde grootte van 10^{-5}) hebben en zijn daarom erg accuraat.

De associatie met opsporing is één van de redenen dat de maatschappelijke acceptatie van vingerafdrukken als biometrisch kenmerk niet optimaal is. Een ander bezwaar van het gebruik van vingerafdrukken is dat personen deze in grote mate achterlaten (residual fingerprints). Indien een grootschalig systeem gebaseerd op vingerafdrukken biometrie in de verkeerde handen is gevallen kunnen de bewegingen van personen in theorie herleid worden. Tot slot vinden gebruikers het soms om hygiënische redenen niet prettig fysiek contact te maken met een vingerprint sensor.

Hoewel vingerafdruk biometrie al ruim 15 jaar oud is, was er tot voor kort weinig publiek bekend over de moeilijkheid om een vingerafdruk sensor te misleiden met een kopie van een vingerafdruk dat wordt geaccepteerd als zijnde afkomstig van de

legitieme gebruiker. Drie jaar geleden is publiekelijk bekend geworden dat het met relatief eenvoudige middelen mogelijk is om gelatine vervalsingen (‘gummy fingers’) van vingerafdrukken te maken die geplakt kunnen worden op een vingertop en waarmee veel vingerafdruk sensors misleid kunnen worden. Zie [I.], [L.]. Dergelijke vervalsingen kunnen worden gemaakt op basis van een (residual) vingerafdruk van de gebruiker, dat wil zeggen zelfs zonder diens toestemming of weten. Daar het vergaren van iemands vingerafdruk in het algemeen niet bijzonder moeilijk is, is bescherming tegen misleiding van een biometrisch systeem op basis van vingerafdrukken (in sommige omstandigheden) een belangrijk aandachtspunt, zie ook Sectie 6.2.

Volgens [M.] biedt visuele inspectie van de vinger, bijvoorbeeld door een medewerker van de Koninklijke Marechaussee op een vliegveld maar een beperkte kans op detectie van het gebruik van ‘gummy fingers’. Zelfs indien de toezichthouder goed wordt geïnstrueerd, wordt de kans op visuele detectie van ‘gummy fingers’ door [M.] op slechts 70% ingeschat. Slechts betasting van de vingertop door een toezichthouder biedt voldoende bescherming tegen ‘gummy fingers’.

Dit is de reden dat sommige van dergelijke systemen gebruik maken van ‘live and well’ detectie. Hiermee wordt geclaimd dat het systeem kan vaststellen dat de vingerafdruk behoort bij een ‘levend’ persoon. Dit soort detectie, bijvoorbeeld gebaseerd op het waarnemen van een hartslag in de vinger, is in de praktijk lastig te realiseren.

5.2 Iris patroon (‘iris scan’)

De iris, of het regenboogvlies, is het gekleurde vlies waarin zich het pupil (het schijnbaar zwarte gedeelte van het oog) bevindt. De iris heeft verschillende, goed te bepalen kenmerken zoals bepaalde vlekjes, ringen, radiale en andere strepen die een complex patroon vormen dat uniek is voor elk mens, zelfs voor eeneiige tweelingen. Het patroon van de iris stabiliseert in de eerste twee levensjaren van een mens volgens de literatuur en wijzigt daarna niet meer. Het bedrijf Iridian (http://www.iridiantech.com) is een van de belangrijkste ontwikkelaars van biometrische systemen gebaseerd op iris patronen en heeft op dit terrein een belangrijk octrooi.

Meestal is niet de hele iris zichtbaar bij een persoon; de boven- en onderkant bevinden zich immers meestal onder het ooglid. Biometrische systemen richten zich dus met name op het midden van de iris. Het bepalen van de iris kenmerken (‘iris scan’) geschiedt met een CCD camera tot één meter waarbij het oog wordt verlicht. Dit is vrij ver weg en wordt daarom door gebruikers over het algemeen niet als onprettig ervaren. Het verlichten gebeurt met Near Infra Red (NIR) licht (700-900 nanometer) omdat daarmee de irispatronen het beste zichtbaar kunnen worden gemaakt. Licht van dit type dat of een rode indruk (rond de 800 nanometer) maakt of zelfs onzichtbaar is voor de mens, is in principe ongevaarlijk. Anders dan bij ‘retinal scans’ (zie beneden) wordt bij het bepalen van het iris patroon dus geen gebruik gemaakt van laser licht waarmee het echter toch vaak negatief wordt geassocieerd. Om bij de meting te zorgen dat de positie van het oog ten opzichte van de camera correct is, wordt bijvoorbeeld gebruik gemaakt van een oranje/rood lichtpuntje dat gebruiker alleen ziet in de juiste positie en dat van kleur verandert (groen) als de bepaling is afgerond. Voor het bepalen van iris kenmerken is weinig training nodig voor gebruikers daar de meting vrij passief kan worden uitgevoerd. Slechts een kleine

fractie personen beschikt niet over een (bruikbaar) iris patroon, externe invloeden zoals beroep en leeftijd zijn daarbij van weinig invloed. Biometrische systemen op basis van iris patronen kunnen een erg lage FMR (orde grootte 10^{-5} of zelfs nog kleiner) hebben en zijn dus erg accuraat.

Zoals eerder gesteld, wordt door gebruikers vaak gedacht dat de iris scan gebruik maakt van laser licht hetgeen dus niet het geval is. Indien de gebruikers hierover goed worden geïnformeerd zal het gebruik er van op dit punt als weinig belastend ervaren kunnen worden. Een ander potentieel bezwaar van gebruikers kan zijn dat het iris patroon inzicht geeft in de medische toestand van zijn eigenaar - de (pseudo-)wetenschap Irisscopie is zelfs gebaseerd op deze gedachte - zodat het laten bepalen daarvan privacy gevoelig zou zijn.

Biometrie op basis van iris patronen is minder dan 10 jaar operationeel. Tot zover lijkt het erg moeilijk om een iris bijvoorbeeld chirurgisch aan te passen zodat een iris sensor moeilijk is te misleiden. Het gebruik van kunstmatige irissen via bijvoorbeeld contactlenzen is eenvoudig te detecteren. Een ‘live and well’ detectie is bij iris biometrie conceptueel eenvoudig; bij feller licht vernauwt de pupil en dat kan eenvoudig gedetecteerd worden. De snelheid en mate van vernauwing kan daarbij ook als maat worden gebruikt of de gebruiker gedrogeerd of onder stress staat.

5.3 Retina patroon (‘retinal scan’)

Bij het maken van kleurenfoto’s waarbij geflitst wordt, worden bij gefotografeerde mensen soms ‘rode ogen’ zichtbaar. Dit zijn de bloedvaten op het netvlies (retina), de achterzijde van het oog. Deze bloedvaten hebben een zeer complex patroon dat uniek is voor een mens en dat over het algemeen stabiel is tijdens zijn leven; er bestaan echter zeldzame ziekten die een verandering kunnen geven op het patroon. Het patroon van de bloedvaten op het netvlies kan worden bepaald door het netvlies te belichten en hiervan een opname (‘retinal scan’) te maken met een camera op 6-8 cm afstand. Voor de verlichting van het netvlies wordt gebruik gemaakt van zwak laserlicht in het infrarood gebruikt. Laser licht is monochromatisch (éénkleurig) licht waarvan de golven allemaal in dezelfde fase zijn en in de zelfde richting gaan zodat het nauwelijks verstrooid. Laserlicht kan vergeleken worden met een waterstraal die sterk gebundeld is, terwijl gewoon licht een soort tuinsproeier is. Dit betekent dat als de laserbron erg sterk is dat dan ook de bundel, zelfs over grote afstand, in staat is hoge energie af te geven op het verlichte object waarbij dit zelfs verbrand kan worden.

Slechts een kleine fractie personen beschikt niet over een (bruikbaar) retina patroon, externe invloeden zoals beroep en leeftijd zijn daarbij van weinig invloed hoewel sommige zeldzame ziekten wel een invloed kunnen hebben op het patroon. Hoewel biometrie op basis van retina patronen relatief nieuwe commerciële technologie is, wordt zij door sommigen als de meest accurate gezien en een erg lage FMR (orde grootte 10^{-5} en kleiner) lijkt goed haalbaar te zijn. Uiteraard wordt bij retinal scans gebruik gemaakt van zwakke (veilige) lasers, maar het gebruik ervan wordt door gebruikers toch als belastend ervaren. Dit wordt nog versterkt doordat de gebruiker zijn oog dicht bij de apparatuur (6-8 cm) moet plaatsen. Hierbij is wel enige training nodig. Evenals bij iris patronen wordt ook soms gesuggereerd dat retina patronen inzicht geven in de medische toestand van de eigenaren zodat het laten bepalen daarvan privacy gevoelig zou zijn. De eerste retinal scan systemen werden rond 1985 op de markt gebracht door de firma EyeDentify maar werden voor deze datum al

ingezet voor militaire toepassingen. Hoewel de commerciële systemen dus nog een relatief nieuw zijn, lijkt een dergelijke sensor moeilijk te misleiden doordat een retina patroon erg moeilijk is te vervalsen, mogelijk wel het allermoeilijkst van alle nu bekende biometrische kenmerken. Het gebruik ervan is overigens duur in vergelijking met vingerafdruk en iris biometrie, zie Sectie 6.7.

5.4 Gezichtspatroon

Identificatie van personen door mensen zelf vindt vaak plaats op basis van het gezicht. Het gezicht kent allerlei specifieke attributen op basis waarvan identificatie in principe kan plaatsvinden, zoals de relatieve locatie en vorm van het hoofd, de ogen, wenkbrauwen, neus, lippen en kin enzovoort. Het vastleggen van gezichtkenmerken ter latere identificatie gebeurt al jaar en dag door opsporingsdiensten door het maken van een pasfoto van een verdachte, vaak in combinatie met het vastleggen van diens vingerafdrukken. De kenmerken van het gezicht zijn niet bijzonder uniek voor een mens, denk daarbij bijvoorbeeld aan eeneiige tweelingen. Daarbij kan het gezicht van een mens tijdens zijn leven veranderen.

Bij een biometrische toepassing wordt met een standaard (goedkope) zwart-wit camera de gebruiker op een meter afstand of minder gescand. Hierna lokaliseert het systeem het gezicht van de gebruiker en wordt het beeld voor het systeem genormaliseerd, dat wil zeggen indien noodzakelijk wordt het beeld geschaald en geroteerd en wordt het contrast aangepast om binnen de parameters van het systeem te passen. Vervolgens wordt het digitale biometrische template bepaald. Door de vele gemoedstoestanden die het gezicht kent en door invloeden als lichtval, is het eenduidig vastleggen van een gezicht echter niet eenvoudig. Dit wordt verder beïnvloed door zaken als positie van het hoofd, lichtval en achtergrond bij het bepalen van het beeld. Ook zaken als haardracht (lang haar) en brillen kunnen moeilijkheden opleveren. Gezichtsherkenning wordt niet als een bijzonder accuraat gezien, eeneiige tweelingen kunnen bijvoorbeeld veelal niet worden onderscheiden. De typische FMR bij gezichtsherkenning ligt rond de 10^{-3} hetgeen niet conform is met de eis uit ANSI X9.84. Slechts een zeer kleine fractie personen zal geen bruikbare gezicht kenmerken hebben voor deelname binnen een daarop gebaseerd biometrisch systeem. Gezichtsherkenning heeft van alle biometrische systemen een hoge gebruikersacceptatie waarschijnlijk omdat het scannen lijkt op het nemen van een pasfoto. In een onderzoek van het College Bescherming Persoonsgegevens (CBP) wordt aangegeven dat gezichtskenmerken en de daarop gebaseerde templates mogelijk bijzondere persoonsgegevens zijn conform de Europese privacy richtlijn 95/46/EC omdat hieruit mogelijk informatie kan worden herleid over iemands ras.

Sommige gezichtsherkenning systemen kunnen worden misleid doordat een foto op ware grootte van een legitieme gebruiker voor het gezicht van de aanvaller wordt gehouden. Ook plastische chirurgie kan resulteren in misleiding van een gezichtsherkenning systeem. Gezichtsherkenning wordt daarom niet als bijzonder fraudebestendig gezien.

5.5 Infrarood gezichtspatroon

Evenals het hiervoor besproken gezichtsherkenning is ook dit type biometrie gebaseerd op het gezicht. Het verschil is echter dat bij infrarode gezichtkenmerken gelet op wordt op het patroon van bloedvaten onder de gezichtshuid. Dit patroon wordt bepaald aan de hand van een thermogram waarin de warmteverschillen in het

gezicht zijn aangegeven: een bloedvat is warmer dan zijn omgeving. Het wordt aangenomen dat het bloedvatenpatroon onder de gezichtshuid een uniek kenmerk voor mensen is, hoewel dit nog niet voldoende onderbouwd is. Naar verluidt wordt dit bloedvatenpatroon zelfs niet veranderd door (oppervlakkige) plastische chirurgie, hetgeen een voordeel boven biometrie op gewone gezichtskenmerken betekent. Het patroon kan wel veranderen indien het gezicht fors dikker of dunner wordt.

Het thermogram benodigd voor het bepalen van het biometrische template wordt zichtbaar gemaakt door een beeld te maken van het gezicht met een infrarode camera. Hiervoor is geen additionele verlichting noodzakelijk en kan daarom zelfs in het donker plaatsvinden. Evenals gewone gezichtsherkenning zal slechts een zeer kleine fractie personen niet geschikt zijn voor een deelname in een biometrisch systeem gebaseerd op infrarode gezichtskenmerken. Over de accuraatheid van dergelijke systemen is ons weinig bekend. Het lijkt ons echter in principe mogelijk om met dit type systemen een FMR van 10^{-4} of beter te bereiken zoals geëist vanuit ANSI X9.84. Infrarode gezichtsherkenning heeft evenals gewone gezichtsherkenning één van de hoogste gebruikersacceptaties waarschijnlijk omdat het scannen lijkt op het nemen van een pasfoto. Naar wordt aangenomen heeft infrarode gezichtsherkenning een hoge bestendigheid tegen misleiding in ieder geval substantieel hoger dan de misleidingbestendigheid van gewone gezichtsherkenning.

5.6 Handtekening

Identificatie van personen in juridische documenten zoals contracten door mensen zelf vindt plaats op basis van een geschreven handtekening gebaseerd op de unieke karakteristieken van iemands handschrift. Hoewel dit gebruik van de handtekening erg oud is, is het niet feilloos. Handtekeningen van verschillende personen zullen zelden op elkaar lijken, maar ook twee handtekeningen van dezelfde persoon zijn niet exact hetzelfde en zeker als er enige tijd tussen het plaatsen daarvan zit. Een handtekening kan ook veranderen met de jaren.

Biometrische systemen gebaseerd op geschreven handtekeningen hebben in principe weinig te maken met de digitale handtekening gebaseerd op publieke sleutel cryptografie. In theorie kan een biometrisch handtekening systeem worden gebruikt als identificatie vooraleer de private signeer sleutel kan worden gebruikt om een elektronische handtekening te plaatsen op elektronisch document. Vaak wordt hier echter een wachtwoord of PIN code (smartcard) voor gebruikt. Er zijn twee typen biometrische systemen gebaseerd op geschreven handtekeningen. Het eerste type (‘statische’) vellen hun oordeel op het eindresultaat, de handtekening, net zoals mensen dat doen. Dergelijke systemen letten op de vormen in de handtekening zoals specifieke krullen. Dynamische typen systemen richten zich niet op het eindresultaat (de handtekening) maar op de dynamiek van het proces waarin het gezet wordt: richtingen van bewegingen, versnellingen, onderbrekingen en uitgeoefende druk. Beide type systemen maken gebruik van een sensor (‘handtekening tableau’) waarbij de gebruiker met een (speciale) pen zijn handtekening moet plaatsen. De sensor legt daarbij de exacte positie van de penpunt en daarmee van de handtekening vast. Belangrijke producenten van biometrische systemen op basis van de handtekening zijn Cybersign (www.cybersign.com), Penop (www.penop.com) en Quintet. Biometrische systemen gebaseerd op handtekeningen worden niet als bijzonder accuraat gezien, de FMR ligt rond de $5*10^{-2}$ en hoger. Niet alle personen beschikken

over een handtekening, waarbij met name gedacht kan worden aan jonge personen (<12 jaar).

Hoewel het gebruik van handtekeningen bij het aangaan van contracten maatschappelijk geaccepteerd is, is het gebruik daarvan in een biometrische context minder geaccepteerd. Een bezwaar van gebruikers kan zijn dat de eigenaar van het systeem de geplaatste handtekeningen kan misbruiken door hiermee contracten aan te gaan in de hun naam. In hoeverre dit een steekhoudend argument is, is onduidelijk maar feit is dat verschillende koeriersdiensten als sinds geruime tijd van ontvangers verlangen dat zij hun handtekening als ontvangstbevestiging plaatsen op een digitaal handtekening tableau. Hoewel het eerder genoemde bezwaar hier ook op van toepassing is, stuit dit blijkbaar toch niet op grote weerstand.

De fraude bestendigheid van handtekening herkenning wordt niet als erg hoog bestempeld. Gesteld kan echter worden dat de fraude bestendigheid van dynamische systemen hoger is dan statische systemen, ook al omdat het ‘stelen’ van een template in een dynamisch systeem moeilijker is dan bij een statisch systeem.

5.7 Stem

Mensen zijn vaak erg goed in het identificeren van personen aan de hand van hun stem. Het menselijk stemgeluid wordt geproduceerd door trillingen in de stembanden die zich in het strottenhoofd bevinden (ongeveer 80 keer per minuut bij mannen en 400 keer per minuut bij vrouwen). Het uiteindelijke geluid dat gehoord wordt, wordt ondermeer bepaald door de karakteristieken van het strottenhoofd, stembanden, neusholten, mond en lippen. Het stemgeluid van een mens is niet bijzonder onderscheidend en varieert tijdens diens levensloop met als extreem voorbeeld het verlagen van de mannelijke stem tijdens de pubertijd. Ook externe invloeden (verkoudheid, overmatig stemgebruik) kan de karakteristieken van het stemgeluid tijdelijk veranderen.

Er zijn twee typen biometrische systemen gebaseerd op het stemgeluid. Bij het eerste type (‘tekst afhankelijk’) dient de gebruiker een aantal woorden uit te spreken die vooraf zijn vastgelegd als onderdeel van een veel grotere selectie. Bij tweede type (‘tekst onafhankelijk’) is werking van het systeem onafhankelijk van de uitgesproken frase. De bepaling is in beide gevallen erg gevoelig voor achtergrondgeluid. Het biometrisch template wordt bepaald op basis van zaken als toonhoogten, energie patroon, vorm van de geluidsgolven en dergelijke. Stemherkenningsystemen hebben een ongunstig hoge FMR (0.1) en worden daarom niet als erg accurate systemen beschouwd. Niet alle personen kunnen gebruik maken van stemherkenningsystemen bijvoorbeeld omdat zij niet kunnen lezen en zo de gewenste woorden niet kunnen uitspreken. Het gebruik van stemherkenning heeft wel een hoge acceptatie graad onder gebruikers. De fraude bestendigheid van stemherkenningsystemen is niet bijzonder hoog, zo hebben goede imitators een goede kans om dergelijke systemen te misleiden.

5.8 Hand geometrie

De menselijke hand heeft diverse karakteristieke geometrische kenmerken, zoals de vorm van de hand, de lengte van de vingers en de locatie van de knokkels. Biometrische systemen op basis van hand geometrie maken een template op basis van deze kenmerken. Het onderscheidend vermogen van dergelijke kenmerken scoort

gemiddeld in het geheel van alle biometrische kenmerken en is zeker niet optimaal. Hetzelfde geldt voor permanentie: hand geometrie blijft redelijk stabiel tijdens de levensduur van een volwassen persoon; tijdens de kindertijd is de hand geometrie verre van stabiel. Belangrijke producten van biometrische systemen op basis van hand geometrie zijn Recognition Systems (www.recogsys.com) en Biomet Partners (www.biomet.ch). Hand geometrie biometrie werd grootschalig ingezet tijdens de Olympische Spelen in Atlanta in 1996.

Bij het bepalen van de hand geometrie dient de gebruiker zijn hand in een mal te plaatsen waarin door één of meer pinnen de plaats van de vingers wordt aangegeven. Vervolgens wordt een, soms driedimensionaal, beeld van de hand vastgelegd door een camera waarbij de pinnen het systeem een eerste aanwijzing geven van de locatie van de vingers en dergelijke. Biometrische systemen gebaseerd op hand geometrie worden als gemiddeld accuraat gezien, de FMR ligt rond de 10^{-3}. Niet alle personen beschikken over een gave hand en sommige ziekten zoals bijvoorbeeld artritis kunnen problemen geven bij het gebruik van biometrie op basis van hand geometrie.

De maatschappelijke acceptatie van hand geometrie is gemiddeld. Een belangrijk bezwaar van gebruikers kan hygiëne zijn als veel gebruikers dezelfde sensor moeten gebruiken. Dit bezwaar kan nog verder toenemen als deze sensor zich in een publieke ruimte bevindt die onderhevig is aan vandalisme. De bestendigheid tegen misleiding van hand geometrie biometrie wordt als gemiddeld gezien.

5.9 Hand bloedvaten patroon

Evenals het hiervoor besproken hand geometrie is ook dit type biometrie gebaseerd op kenmerken van de hand. Bij hand bloedvaten biometrie wordt gelet op het patroon van bloedvaten onder de huid van de bovenkant van de hand. Dit patroon wordt bepaald aan de hand van een opname met een infrarode camera. Het wordt aangenomen dat het bloedvatenpatroon onder de huid van de hand een uniek kenmerk voor mensen is, hoewel dit nog niet voldoende onderbouwd is. Ziekten en ouderdom kunnen het bloedvaten patroon verstoren. Biometrische systemen op basis van het hand bloedvaten patroon worden ondermeer geproduceerd door BK systems.

Bij het bepalen van het hand bloedvaten patroon dient de gebruiker zijn hand in een mal te plaatsen waarin door één of meer pinnen de plaats van de vingers wordt aangegeven. Vervolgens wordt een infrarood beeld van de hand vastgelegd door een camera waarbij de pinnen het systeem een eerste aanwijzing geven van de locatie van de vingers en dergelijke. Hand bloedvaten biometrie is weliswaar accurater dan hand geometrie biometrie maar wordt toch niet gezien als erg hoog. Wij konden weinig gedocumenteerde gegevens over dit punt vinden. De acceptatie van hand bloedvaten biometrie is ongeveer gelijk aan die van hand geometrie biometrie. De bestendigheid tegen misleiding van hand bloedvaten biometrie wordt als hoog gezien.

6 Een indeling van de belangrijkste criteria voor biometrische systemen

Tijdens de bespreking van de diverse biometrische technieken hebben we reeds impliciet een aantal belangrijke prestatie criteria genoemd. In deze sectie zullen we deze criteria expliciet benoemen.

6.1 Maatschappelijke acceptatie

Dit is de mate waarin de biometrische techniek wordt geaccepteerd door het grote publiek. Voldoende acceptatie is noodzakelijk voor het slagen van een biometrische systeem in de praktijk en hangt af van verschillende factoren waaronder:

- Ingrijpendheid van gebruik ('invasiveness')
  Het bepalen van sommige biometrische kenmerken wordt door gebruikers als te ingrijpend gezien. Een voorbeeld hiervan is de retinal scan waarbij het netvlies met een zwakke laserstraal wordt belicht waarbij de gebruiker zijn oog op korte afstand van de sensor moet houden.
- Privacy
  In uitspraken van en onderzoeken ([D.], [E.]) uitgevoerd door het College Bescherming Persoonsgegevens (CBP) wordt aangegeven dat biometrische gegevens in beginsel beschouwd dienen te worden als persoonsgegevens in de zin van artikel 1 van de Wet Bescherming Persoonsgegevens (WBP) en de Europese privacy richtlijn 95/46/EC. In het onderzoek [E.] uitgevoerd door het CBP wordt zelfs aangegeven dat sommige biometrische kenmerken en daarop gebaseerde templates bijzondere persoonsgegevens kunnen zijn in de zin van de Europese privacy richtlijn 95/46/EC omdat hieruit mogelijk informatie kan worden herleid over iemands ras of gezondheid. De verwerking en opslag van bijzondere persoonsgegevens dienen aan een nog strenger beveiligingsregime onderworpen te zijn dan gewone. Dit is verder bekrachtigd door het CPB in een uitspraak over de zogenaamde Discopas ([D.]) in 2001. De Discopas is een onderdeel van een biometrisch toegangscontrolesysteem dat een bedrijf op de markt wilde brengen voor horeca- en sportgelegenheden en dat gebaseerd is op gezicht geometrie en vingerafdrukken. Andere voorbeelden van biometrische kenmerken die mogelijk als bijzondere persoonsgegevens gezien kunnen worden, zijn de iris en retina patronen daar deze dicht tegen medische gegevens aanzitten. Op basis van het iris patroon is zelfs een (pseudo-) medische wetenschap gebaseerd (iriscopie). Een ander, en extreem, voorbeeld van een biometrisch kenmerk dat zeker als bijzonder persoonsgegeven kan worden bestempeld is het DNA kenmerk van mensen. Mede om deze reden hebben we het DNA kenmerk ook niet behandeld als biometrische authenticatie techniek.

  Bij de vraag of biometrische templates die afgeleid zijn van biometrische kenmerken die als bijzondere persoonsgegevens zijn bestempeld, ook bijzondere persoongegevens zijn, speelt de vraag of uit de templates de oorspronkelijke kenmerken (foto gezicht, afbeelding iris) kunnen worden 'teruggerekend' waaruit informatie kan worden herleid over iemands ras of gezondheid. Vaak wordt door biometrie fabrikanten gesteld dat dit terugrekenen niet mogelijk is. In het eerder genoemde 'Discopas' onderzoek concludeerde het CBP echter dat de hierbij gebruikte gezicht geometrie algoritmen kunnen worden teruggerekend zodat uit het template de oorspronkelijke scan kan worden herleid. In beginsel [E.] sluit het CBP niet uit dat biometrische templates die afgeleid zijn van biometrische kenmerken die als bijzondere persoonsgegevens zijn bestempeld, dit zelf niet hoeven te zijn.

  Zelfs als dit terugrekenen niet kan, dan nog kleven er toch privacy aspecten aan biometrische templates. Zo zijn (en blijven) templates in theorie immers uniek voor een persoon en kunnen zij in principe worden misbruikt om personen te identificeren zonder dat de persoon daar toestemming voor gegeven heeft of zelfs

kennis van heeft. Daarbij komt dat het bij sommige biometrische kenmerken (zoals vingerafdrukken) relatief eenvoudig is om uit sporen of observatie biometrische kenmerken te bepalen die vervolgens, weliswaar met enige moeite, kunnen gebruikt om geregistreerde personen te monitoren en op te sporen. In het document [E.] stelt het CBP enkele vragen waarvan de beantwoording de basis kan vormen voor de verantwoorde inzet van biometrische authenticatie:

a. Welke biometrische gegevens zijn echt nodig voor het doel en is het gebruik hiervan proportioneel?
b. Worden de gegevens rechtmatig ingewonnen? Is de betrokken persoon geïnformeerd?
c. Is er sprake van 'bijzondere gegevens'?
d. Wat gebeurt er met de oorspronkelijke biometrische gegevens? Worden deze verwijderd?
e. Zijn de biometrische gegevens zo opgeslagen dat ze niet meer terug te voeren zijn tot de oorspronkelijke gegevens?
f. Is het mogelijke om de meting van de gegevens en de verificatie decentraal te laten plaatsvinden?
g. Is de beveiliging van templates voldoende?
h. Rechtvaardigt het doel een eventuele centrale opslag van biometrische gegevens?

- Hygiëne
  Soms vergt een biometrisch systeem dat de gebruikers fysiek contact maken met een sensor dat zich in het publieke domein bevindt. Deze sensor zal door velen worden gebruikt en kan daardoor vies kan worden. Een voorbeeld hiervan is biometrie op basis van hand geometrie.
- Eenvoud van gebruik

6.2 Fraudebestendigheid

Dit is de mate waarin een biometrisch systeem gevoelig is voor fraude, met name bij identificatie en verificatie. Omdat biometrische kenmerken in principe niet als geheim beschouwd kunnen worden gehouden is het van belang dat de partij die vertrouwt op de biometrische authenticatie voldoende zekerheid heeft dat de componenten van een biometrisch systeem en de communicatie daartussen vrij van manipulatie zijn. We onderscheiden de volgende scenario's (zie onderstaand diagram):

A. Misleiding van de Sensor
Bij dit type fraude richt de aanvaller zich op het produceren van een falsificatie van het biometrische kenmerk en dat vervolgens wordt aangeboden aan de sensor van het systeem. Een voorbeeld hiervan zijn de ‘gummy fingers’, gelatine falsificaties van vingerafdrukken, zoals besproken in Sectie 5.1. De bescherming tegen dit type fraude is sterk afhankelijk van het type biometrische technologie dat wordt gebruikt maar ook van de toezicht van partij die op het biometrisch systeem vertrouwt, kan uitoefenen op de gebruikers bij het scannen van de kenmerken. Ter illustratie, bij het gebruik van vingerafdruk biometrie bij grenscontrole waarbij de gebruiker onder toezicht van de Koninklijke Marechaussee zijn vinger op de sensor dient te leggen, zullen ‘gummy fingers’ minder kans van slagen hebben. Bescherming tegen sensor misleiding kan verder versterkt worden door ‘live and well’ beschermingstechnieken zoals additionele sensors die meten of in de vinger waarvan de vingerafdruk wordt bepaald ook een hartslag is waar te nemen. Ook de reactie van de iris op lichtverschillen is een voorbeeld van een “live and well” detectie en wel bij een iris scan. Retinal- en de iris scan lijken intrinsiek het minst vatbaar voor dit type fraude.

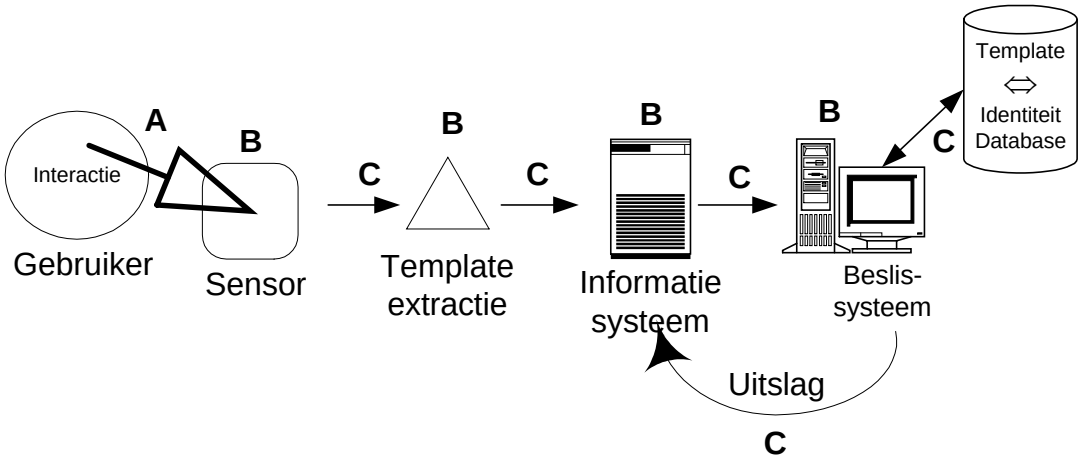
B. Manipulatie van componenten
Dit type fraude tracht de interne verwerking van één der componenten van een biometrisch systeem te manipuleren zodat het eindresultaat een foutieve verificatie of identificatie is. Een voorbeeld hiervan is een aanvaller die ‘kwaadaardige code’ weet te plaatsen op het beslissysteem dat er voor zorgt dat er altijd een positieve verificatie naar het informatiesysteem wordt gestuurd. Ter illustratie, bij toegangsbeveiliging tot smartcards op basis van vingerafdrukken (zie Sectie 4.2) wordt de template extractie en het nemen van de beslissing wordt vaak om redenen van performance in software op de PC uitgevoerd; het beslissingsysteem notificeert de smartcard via een seriële verbinding over zijn beslissing. Reverse engineering en aanpassen van de software biedt een aanvaller de mogelijkheid de feitelijke biometrische vergelijking te omzeilen.

Bescherming tegen dit soort fraude kan gevonden worden in fysieke controle en toezicht op de componenten, het plaatsen van de componenten in goed beveiligde (‘hardened’) computersystemen of zelfs ‘trusted devices’ zoals smartcards. Om het eerste punt te illustreren met het eerder genoemde voorbeeld van grenscontrole: de Koninklijke Marechaussee laat niet toe dat grenspassanten de software van het biometrische systeem kunnen aanpassen.

C. Manipulatie van de communicatie tussen componenten
Dit type fraude tracht de communicatie tussen de diverse componenten van een biometrisch systeem stop te zetten (‘denial of service’) of te manipuleren. Een voorbeeld hiervan is het plaatsen door een aanvaller van een signaal op het communicatiekanaal tussen de sensor en de extractor te plaatsen dat correspondeert met dat van een legitieme gebruiker en dat bijvoorbeeld eerder is afgeluisterd op dit of een ander kanaal. Dit type aanval kan bijvoorbeeld worden toegepast indien een losse vingerafdruk lezer is verbonden met een PC waar software de extractie verzorgt en waarbij ‘kwaadaardige code’ het seriële kanaal tussen de lezer en de software afluistert. In zijn algemeenheid kan dit risico optreden indien biometrische authenticatie ‘op afstand’ wordt gebruikt, bijvoorbeeld via het Internet.

Bescherming tegen dit type fraude kan gevonden worden in:

- Fysieke controle en toezicht op de componenten en de communicatie daar tussen.
- Een ‘trusted path’ tussen de componenten of door componenten te integreren in ‘trusted’ devices. Vergaande voorbeelden hiervan zijn de smartcards waarin vingerafdruk lezer en vingerafdruk template extractor zijn geïntegreerd (vergelijk de smartcards van Idtek, www.idtek.com) en waarbij het resultaat dat wordt gestuurd uit de smartcard uitgerust is met een Message Authentication Code (MAC) gebaseerd op geheime sleutel cryptografie op of met een digitale handtekening gebaseerd op publieke sleutel cryptografie, geproduceerd met een cryptografische sleutel die (veilig) wordt bewaard in de smartcard.
- Een ‘trusted path’ gebaseerd op cryptografie, waarmee echter niet de beschikbaarheid van de verbinding tussen de componenten kan worden gegarandeerd.



6.3 Universaliteit

Universaliteit is het percentage personen uit de gebruikersdoelgroep waarvoor het biometrisch kenmerk voldoende eenduidig bepaald kan worden. Er zijn twee typen gebruikers waarvoor het biometrisch kenmerk niet voldoende eenduidig bepaald kan worden:

1. Personen die niet over het biometrische kenmerk beschikken. Bij vingerafdruk biometrie zijn dit voorbeeld personen die bepaalde vingers missen.
2. Personen die weliswaar over het biometrische kenmerk beschikken, maar om een of andere, vaak onduidelijke, reden niet in staat zijn dit succesvol te laten bepalen. Dit type gebruikers worden ook wel ‘outliers’ genoemd.

Geen enkele biometrisch kenmerk heeft een universaliteit van 100%, hetgeen in de praktijk betekent dat er altijd een (beperkte) alternatieve authenticatie methode moet zijn in aanvulling op de biometrische, dit kan ook een biometrische zijn. Er dient wel gewaakt te worden dat de alternatieve authenticatie methode vergelijkbaar sterk is als de biometrische en geen zwakheid introduceert. De Failure to Enroll (FTE) waarde voor een biometrisch systeem is het percentage outliers als deel van personen met het biometrische kenmerk, of anders gezegd de kans dat een gegeven persoon met het kenmerk toch niet geregistreerd kan worden. Kenmerken met een hoge universaliteit zijn: retinal scan, iris scan en (infrarode) gezichtsherkenning.

6.4 Accuraatheid

Dit is de mate waarin een biometrisch systeem feilloos werkt, hetgeen wordt uitgedrukt in het kunnen behalen van lage FMR, FNMR en EER waarden. Zie Sectie 4. De accuraatheid in termen van de FMR waarde van de diverse kenmerken worden besproken in de sectie waarin ze worden besproken en zijn gebaseerd op [C.] en [N.]. Wij noemen slechts de FMR waarde omdat de ANSI X9.84 standaard hier eisen aanstelt. Een FMR waarde zegt overigens niet zoveel zonder FNMR waarde, mogelijk dat daarom de FMR gegevens van beide genoemde bronnen niet altijd consistent zijn. Het is erg lastig om objectieve en volledige gegevens te krijgen over de accuraatheid van biometrische systemen en de in dit artikel genoemde FRM waarden zijn daarom slechts indicatief bedoeld. De International Biometric Group (www.ibgweb.com) biedt naar verluidt dergelijke gegevens, maar de prijzen van hun rapporten (bijvoorbeeld 5000$ voor een rapport inzake iris biometrie) zijn nogal hoog. Nog los van het feit dat het om budgettaire redenen niet mogelijk was deze rapporten aanschaffen in het kader van het schrijven van dit artikel, is dat ook betrekkelijk zinloos daar de gegevens hieruit niet mogen worden overgenomen. Op de website van deze groep zijn ook gratis rapporten te lezen, zij het dat daar nauwelijks harde gegevens in staan. Opmerkelijke conclusie uit het document http://www.ibgweb.com/cbt_lessons.pdf is dat “Performance as tested [is] almost always worse than performance claimed.”

Dit gebrek aan objectieve en volledige gegevens maakt het erg lastig voor organisaties om een goede haalbaarheidsanalyse uit te voeren inzake het gebruik van biometrie. Ons inziens vormt dit gebrek aan gegevens daarmee in feite een belemmering voor de acceptatie van biometrie in het algemeen. De realisatie van dergelijke gegevens zou ons inziens daarom een grote prioriteit moeten krijgen binnen de biometrische industrie. Leveranciers van biometrische systemen zijn er echter vaak vaak nogal huiverig voor om (niet-anoniem) vergeleken te worden met anderen, vergelijk de test van biometrische systemen gebaseerd op vingerafdrukken op http://bias.csr.unibo.it/fvc2002. Deze houding zal ons inziens moeten veranderen wil de biometrische markt echt volwassen worden.

In onze visie betekent een redelijke accuraatheid dat de minimaal geadviseerde FMR waarde in de ANSI standaard X9.84 (zie [A.]) van 10^{-4} in de praktijk moet kunnen worden behaald. Een hoge accuraatheid betekent dat een FMR van 10^{-5} of kleiner moet kunnen worden behaald in de praktijk. Het feit dat een biometrisch systeem een hoge FMR waarde heeft betekent nog niet dat zij onbruikbaar is voor toepassingen die een hoge accuraatheid eisen. Indien men twee of meer laag accurate biometrische systemen combineert (‘multifactor biometrie’), dat wil zeggen eisen dat een gebruiker door beide systemen wordt geauthenticeerd, zal de corresponderende FMR waarde corresponderen met het product van de FMR waarden zijn van de onderliggende systemen; de FNMR zal de som van de oorspronkelijke FNMR waarden zijn.

6.5 Onderscheidend vermogen

Dit is de mate waarin een biometrisch kenmerk in staat is om verschillende personen te onderscheiden. Anders dan het hiervoor besproken ‘accuraatheid’ zegt onderscheidend vermogen niet iets over de huidige biometrische techniek, maar meer iets over de potentie daarvan: een kenmerk kan uniek zijn voor individuen maar daarmee hoeft het digitale template dat nog niet te zijn, juist omdat getracht wordt dit van beperkte omvang te houden. Kenmerken met een hoog onderscheidend vermogen

zijn vingerafdrukken en de iris en retina patronen. Kenmerken met een laag onderscheiden vermogen zijn (infrarood) gezichts- en stempatronen en de handtekening. Het onderscheidend vermogen van de diverse kenmerken wordt besproken in de sectie waarin ze worden behandeld.

6.6 Permanentie

Dit is de mate waarin een biometrisch kenmerk stabiel blijft tijdens de levensduur van een persoon. Kenmerken met een hoge permanentie zijn vingerafdruk, retinal- en iris patronen. De permanentie van de diverse kenmerken wordt besproken in de sectie waarin ze worden behandeld.

6.7 Complexiteit gebruik

Dit is de mate waarin een biometrisch systeem complex is in gebruik. Belangrijke factoren hierbij zijn: de kosten van de sensor en de grootte templates in bytes.

In onderstaande tabel staan indicaties van deze factoren (ontleend aan [C.]). De kosten van de iris en retina patroon sensors zijn ons inziens wat laag in geschat en zullen meer in de richting van 2.5K EURO liggen. De kosten van de Infrarood gezichtspatroon sensor (50K Euro) lijkt ons wat hoog.

Biometrische Kenmerk	Grootte Template (KiloBytes)	Kosten Sensor (KiloEuro)
Vingerafdruk	0.3	0.2-0.5
Iris patroon	0.4	0.1
Retina patroon	0.05	1.5
Gezichtspatroon	0.25	0.2
Infrarood gezichtspatroon	0.4	50
Handtekening	0.01	0.5
Stem	0.02	> 0.2
Hand patroon	0.009	2.2
Hand bloedvaten patroon	0.05	0.1

6.8 Indicatieve vergelijking

Op basis van de geraadpleegde literatuur (waaronder [C.], [F.]) komen we tot de volgende indicatieve vergelijking tussen de diverse biometrische technieken.

Biometrische Techniek	Maatschappelijke Acceptatie	Fraude Bestendigheid	Universeel-heid	Accuraat-heid	Onderscheidend vermogen	Permanentie	Complexiteit gebruik
Vingerafdruk	Medium	Medium	Medium	Hoog	Hoog	Hoog	Laag
Iris patroon	Medium	Hoog	Hoog	Hoog	Hoog	Hoog	Laag
Retina patroon	Laag	Hoog	Hoog	Hoog	Hoog	Medium	Medium
Gezichtspatroon	Hoog	Laag	Hoog	Laag	Laag	Laag	Laag
Infrarood gezichtspatroon	Hoog	Medium	Hoog	Medium	Medium	Laag	Hoog
Handtekening	Hoog	Laag	Laag	Laag	Laag	Laag	Laag
Stem	Hoog	Laag	Medium	Laag	Laag	Laag	Laag
Hand patroon	Medium	Medium	Medium	Medium	Medium	Medium	Medium
Hand bloedvaten patroon	Medium	Medium	Medium	Medium	Medium	Medium	Laag

7 De belangrijkste standaarden rond biometrische systemen

De bekendste biometrische standaard is BioAPI (zie [B.]) die voor fabrikanten van biometrische modulen een zogenaamde Application Program Interface (API) vastlegt. Deze API stelt programmeurs in staat om op gestandaardiseerde wijze aanroepen te doen naar dergelijke modulen zodat zij zich niet hoeven te verdiepen in de specifieke eigenschappen van de modulen. Zo voert de BioAPI aanroep BioAPI_Verify() een biometrische verificatie uit. Hoewel deze aanroepen dus open zijn gestandaardiseerd zijn de onderliggende algoritmen dat niet. BioAPI is in februari 2002 aangenomen als officiële ANSI standard (ANSI INCITS 358-2002).

Een andere belangrijke biometrische standaard is CBEFF (zie [K.]), de Common Biometric Exchange Framework Format. Deze standaard is ontwikkeld door het Amerikaanse National Institute of Standards and Technology (NIST) en het Biometric Consortium. CBEFF legt een gemeenschappelijk biometrisch bestandsformaat vast waaronder een biometrische header, een biometrisch specifiek datablock en een handtekening blok. CBEFF heeft niet als doel om compatibiliteit te realiseren tussen biometrische systemen van verschillende fabrikanten, maar draagt zorg dat informatiesystemen kunnen vaststellen van welke fabrikant/techniek specifieke biometrische data of randapparatuur afkomstig is. Dit maakt uitwisseling tussen systemen eenvoudig mogelijk. Zowel BioAPI als ANSI X9.84 formateringen zijn opgenomen binnen CBEFF. Het XCBF Technical Committee is bezig om de beschrijvingen uit CBEFF ook te coderen in XML (de Extensible Markup Language), zie http://www.oasis-open.org.

Een derde belangrijke standaard is ANSI X9.84 getiteld “Biometric Information Management and Security for the Financial Services Industry”. Deze standaard definieert eisen voor het beveiligen van biometrische systemen, de biometrische informatie daarin en de communicatie daartussen. ANSI X9.84 gaat verder dan veel andere standaarden in het stellen van kwantitatieve eisen aan beveiliging zoals de eis dat de FMRV en FMRI waarde $\leq 10^{-4}$ dient te zijn en bij voorkeur zelfs $\leq 10^{-5}$. De ANSI X9.84 standaard legt zijn eisen in hoge mate vast in de ASN.1 syntax.

Tot slot willen we nog de ontwikkeling noemen die plaatsvindt binnen ISO in de ontwikkeling van ISO 7816-11 standaard (de eerste 10 onderdelen leggen fysieke en protocollaire aspecten van smartcards, of ICC’s, vast). Binnen het elfde deel van de standaard wordt ondermeer gestandaardiseerd de wijze waarop biometrische templates (‘profielen’) op een smartcard worden opgeslagen, de wijze waarop (inclusief de commando’s) biometrische authenticatie gebruikt kan worden om toegangbeveiliging tot gegevens op de kaart, met name cryptografische sleutels, te realiseren. De ontwikkeling van ISO 7816-11 was in mei 2003 nog niet afgerond.

8 Dankbetuiging

Ik wil de volgende personen graag bedanken voor hun commentaar op een eerdere versie van dit artikel:

- Carlo D’Agnolo
- Marjo Geers (TNO)
- Jeroen Keuning (Atos Origin)
- Ton van der Putte (Atos Origin)

- Hein Kloosterman

De auteur van dit artikel blijft uiteraard als enige verantwoordelijk voor de opinies en eventuele onjuistheden en omissies in dit artikel.

9 Referenties

[A.] American National Standards Institute, *Biometric Information Management and Security*, 27 maart 2001. Zie http://webstore.ansi.org.

[B.] BioAPI Consortium, *BioAPI Specification*, versie 1.1, 16 maart 2001. Zie http://www.bioapi.org.

[C.] Biometric Technology Inc., *Biometric Technical Assessment*, 19 augustus 2002. Zie http://bio-tech-inc.com/Bio_Tech_Assessment.html.

[D.] College Bescherming Persoonsgegevens, Biometrisch toegangscontrolesysteem (discopas), 2001. Zie http://www.cbpweb.nl/documenten/uit_z2000-0080.htm.

[E.] College Bescherming Persoonsgegevens, *At face value*, september 1999. Zie http://www.cbpweb.nl.

[F.] *Code of practice for information security management*, BS ISO/IEC 17799:2000.

[G.] International Biometric Group, *Key Performance Metrics: FMR, FNMR, FTE*, zie http://www.ibgweb.com/reports/public/reports/performance_metrics.html.

[H.] A. Jain et al., *Biometrics: Promising frontiers for emerging identification market*, Comm. ACM, pages 91-98, February 2000. Zie http://www.cse.msu.edu/cgi-user/web/tech/document?ID=436.

[I.] T. Matsumoto et al., *Impact of Artificial "Gummy" Fingers on Fingerprint Systems*, Optical Security and Counterfeit Deterrence Techniques IV, Proceedings of SPIE Vol. #4677, 2002. Zie http://cryptome.org/gummy.htm.

[J.] National Security Agency, *Tokeneer*, December 1997. Zie http://www.biometrics.org/REPORTS/cert_stu_pt2.pdf.

[K.] Biometric Consortium, NIST, *Common Biometric Exchange File Format (CBEF)*, NISTIR 6529, 21 januari 2001. Zie http://www.itl.nist.gov/div895/isis/bc/cbeff/.

[L.] T. van der Putte, J. Keuning, *Biometrical Fingerprint Recognition: Don't Get Your Fingers Burned*, IFIP TC8/WG8.8 *Fourth Working Conference on Smart Card Research and Advanced Applications*, pages 289-303, Kluwer Academic Publishers, 2000. Zie http://www.keuning.com/biometry.

[M.] T. van der Putte, J. Keuning, persoonlijke communicatie, juni 2003.

[N.] SANS Institute, *Biometric Technologies Overview*, 16 maart 2001. Zie http://www.sans.org/rr/authentic/biometric2.php.