De Toekomst van Identificatie zal worden bepaald door:
Biometrie en Paspoort-Smart-Cards!

Lemmens, Kees [0442151] & **Brinkkemper,** Paul [0309729]

De Toekomst van Identificatie zal worden bepaald door: Biometrie en Paspoort-Smart-Cards.

"… Terecht concluderen veel mensen dat er op 11 september 2001 een tijdperk is geëindigd en een nieuw tijdperk is begonnen. Tegenwoordig lijkt voor de beveiligingsindustrie geen geldbedrag te hoog en geen maatregel te gek om de veiligheid te waarborgen "

Brunno de Winter

Inhoud:

Abstract

Dit project verschaft inzicht in diverse biometrische toepassingen zoals vingerafdrukken, gezichtsherkenning, irisscans, en hoe deze toepassingen te gebruiken zijn als identificatiemiddel. Uitvoerig behandelen we het biometrisch paspoort en hoe identiteiten te managen met behulp van nieuwe geavanceerde technologiën en het biometrisch paspoort. Eveneens komen wettelijke aspecten aan bod omstreeks biometrie en beveiliging van persoonsgegevens. Verder gaan we in op standaardisatie en de implementatie van het biometrisch paspoort. Als laatste zullen we onze hoofdvraag beantworden welke is: “In hoeverre kunnen we de identiteit managen met behulp van de unieke menselijke kenmerken verstrekt door een biometrisch paspoort?”.

De Definitie Fase

Inleiding

In deze fase zullen wij een kort de kernbegrippen van ons project behandelen, deze zijn van belang voor een correcte interpretatie van het project.

"Identiteit: de verschillen in onze unieke gedrags, persoonlijke en biometriesche kenmerken die ons op unieke wijze definieerbaar maken"

Identiteit

Identiteit komt van het Oude Franse Woord *identité*, welke op haar beurt weer komt van het Latijnse woord *identitas*. De definities van identiteit: "The distinct personality of an individual regarded as a persisting entity; individuality" (Houghton Mifflin Company, 2003) en: "The set of behavioural or personal characteristics by which an individual is recognized as a member of a group" (Houghton Mifflin Company, 2003) zijn naar onze mening nog niet volledig. Het woord 'uniek' is namelijk niet present. Wij denken dat als we identiteit volledig willen definiëren de definitie er als volgt uit zal moeten zien: *de verschillen in onze unieke gedrag, persoonlijke en biometrische kenmerken die ons op unieke wijze definieerbaar maken.*

Uniek

"Uniek: de enige van zijn/haar soort zijn"

Uniek kunnen we eenvoudig definiëren; uniek is de *enige* van zijn/haar soort zijn; er is dus *geen* gelijke. (O'Neilly, 2003)

Biometrie

"Biometrie: de mogelijkheid om automatisch onze unieke, digitaal meetbare, kenmerken te meten"

Van biometrie zijn een bijzonder groot aantal definities beschikbaar, waarvan de meeste onderling verschillen qua omschrijving. Wij hebben twee definities gekozen die naar onze mening biometrie het beste definiëren, echter ook hier zijn wij van mening dat de gegeven definities niet volledig zijn, daarvoor hebben wij deze twee definities samengebracht in één betere definitie. Naar gelang van Spinella, (2003a): "The word biometrics comes from the Greek language and is derived from the words bio [which means] life and metric [what means measuring] personal characteristics, both physiological and behavioural". De tweede definitie werd verschaft door Blackburn (2003a), "biometrics are 'automated methods of recognizing an individual based on their unique physical or behavioural characteristics.'" Biometrie kan vervolgens worden gedefinieerd als: "de mogelijkheid om automatisch onze unieke, digitaal meetbare, kenmerken te meten". In onze definitie zowel als in de definitie verschaft door Blackburn, stellen wij dat het woord 'automatisch' de identificatie is

voor de toepassing van digitale methoden, dienend voor het vaststellen van een identiteit.

Verificatie, Authentificatie en Identificatie als in een Biometrisch Beveiligings Systeem.

Verificatie kan volgens WebOpedia (2004) worden gedefinieerd als: “the process of comparing a biometric sample against a single reference template of a specific user in order to confirm the identity of the person trying to gain access to the system.”

Authentificatie kan volgens de zelfde bron worden gedifineerd als: “the process of comparing a biometric data sample against all of the system’s databased reference templates in order to establish the identify of a person trying to gain access to the system” (WebOpedia, 2004)

Last but not least, identificatie is het proces van identificeren, ofwel het herkennen van een persoon of ding (O’Neilly, 2003).

Er zijn vereenvoudigd vier soorten van authentificatie en verificatie mogelijk met behulp van biometrie, deze zijn:

1. vingerafdruk scans
2. retina of iris scans
3. spraakherkenning
4. gezichtsherkenning

Identiteit Management

> “… Identity management is the process that manages the complete security-life-cycle for users and network entities in an organization including account creation, suspension, privilege modification, and account deletion”
>
> Stern – 2004d

Dit begrip werd het beste gedefinieerd door Stern (2004d), “identity management is the process that manages the complete security-life-cycle for users and network entities in an organization including account creation, suspension, privilege modification, and account deletion”. Met andere woorden, ‘Identiteit Management’ is meer dan een database gevuld met data, het omvat het gehele proces van af het invoeren van de data tot en met het controleren van een identiteit.

Het paspoort

> “Paspoort: een officieel overheidsdocument waarmee burgers hun nationaliteit en identiteit kunnen aantonen.”
>
> Van Dale

Het Hoofddoel van het Paspoort

Een paspoort is, zoals wij lezen in de dikke Van Dale, een officieel overheidsdocument waarmee burgers hun nationaliteit en identiteit kunnen aantonen. Maar de eisen waaraan het paspoort moet voldoen om de identiteit te kunnen aantonen zijn aan het veranderen.

Ten eerste wordt er volgens T. de Graaf druk vanuit de Verenigde Staten uitgeoefend om biometrische kenmerken in het paspoort op te nemen (2004). Sinds de aanslagen van 11 september 2001 hebben de Verenigde Staten de toegangscriteria tot het land verscherpt en burgers van landen die geen biometrische kenmerken in het paspoort hebben opgenomen of gaan opnemen, kunnen alleen met een visum toegang tot het land krijgen.
Ten tweede is er het dubbelgangerprobleem aan onze eigen grenzen. “Eenderde van de mensen die door die de marechaussee op Schiphol met een onjuist reisdocument worden gepakt, gebruikt een Nederlands paspoort van een ander persoon” (Ravestein, & Zwart, 2004a). Om deze wijze van misbruik tegen te gaan wordt ook gewerkt aan het integreren van vingerafdrukken in paspoorten.

Biometrie

Biometrie; een Inleiding

Anno October 1997, gedurende het door de Gartner Group georganiseerde ITexpo, maakte de heer Gates de volgende mededeling: "*biometric technologies, those that use human characteristics such as fingerprint, will be the most important IT innovations of the next several years*" (Semnerio, 1997). In deze sectie zullen wij nader toelichten waarom wij verwachten dat deze mededeling waar zal zijn.

Enkele duizenden jaren geleden werd er in het oude Egypte al biometrie toegepast als identificatiemiddel. Het was een gewoonte voor de Egyptenaren om personen te identificeren aan de hand van zichtbare kenmerken zoals littekens, ogen en haarkleur, lengte, etc. Het bepalen van de identiteit was van belang voor het toenmalige bedrijfsleven, en ook tegenwoordig is er een grote vraag van organisaties naar betere identificatie middelen (Cherry, 2003a).

Organisaties zijn al sinds de jaren '70 actief bezig met biometrie, in de jaren '70 werd het "Identimat-System" geïntroduceerd bij Shearson Hamill, een WallStreet investeringsorganisatie, dit was tevens het aller eerste identificatiesysteem ooit (DigitalPersona, 1998a).

Tegenwoordig zijn er honderden organisaties die zich bezighouden met biometrie en identificatie. ACG, Imagis, Oracle, Microsoft, Precise Biometrics, NEC, VeriSign en vele anderen. Maar ook de overheden, overal ter wereld, zijn druk bezig om zich betere systemen en identificatiemethoden eigen te maken. Door de eerder genoemde veranderingen als gevolg van de aanslagen van 11 september is de Nederlandse overheid gaan zoeken naar bedrijven die voor hun oplossingen kunnen leveren. Na onderzoek kwamen we er achter dat de volgende vier bedrijven hoofdzakelijk verantwoordelijk zijn voor het biometrische paspoort in Nederland: NEC, Oracle, RSA Security en ACG.

De meest belangrijke biometrische vormen komen aanbod met hun voor- en nadelen. Ook zullen we veel aandacht besteden aan diverse smartcards en identificatie management .

De heer ten Hoorn, sales manager NEC, stond mij op 14 Oktober te woord over de relatie die NEC heeft met de overheid in verband met het biometrisch paspoort. Hij vertelde mij dat zij verantwoordelijk zijn voor het systeem wat de modules via een soort van Virtual index bij elkaar zoekt, Oracle zorgt voor de database toepassingen en RSA security zorgt voor de beveiliging van het Identity Management System. Verder is ACG, met wie ik eveneens gesproken heb, verantwoordelijk voor de smartcards en de smartcardreaders. Wij hadden verwacht dat men gebruik zou gaan maken van de Crypto-Smart-Card, en deze stelling bleek aan de hand van dit gesprek juist te zijn."

Kees Lemmens

Bronnen:
Ruud ten Hoorn (NEC)
René van Ryt (ACG)

Biometrie; Vingerafdrukherkenning

Veel mensen veronderstellen dat het gebruik van vingerafdrukken voor identificatie een nieuwe technologie is, echter het eerste gebruik van vingerafdrukken voor indentificatie stamt uit China. In de 2de eeuw vChr maakten de Chinezen al intensief gebruik van vingerafdruk gebaseerde indentificatie. De zender van een belangrijk document kon worden geverifieerd door zijn vingerafdruk, de afdruk moest overeenkomen met een waxe verzegeling. Het feit dat vingerafdrukken uniek waren voor ieder individu en daarvoor kon worden gebruikt voor accurate indentificatie werd bekend in de 17de eeuw. In de 19de eeuw werd voor het eerst een systeem geintroduceerd die het mogelijk maakte om een zeker individu automatisch te koppelen aan de juiste vingerafdruk. Het Henry classificatie systeem is zo'n systeem welke is gebaseerd op het vergelijken van patronen zoals lussen en spiralen, dit idee wordt vandaag de dag nog steeds gebruikt, het was ontwikkeld door een Brit, genaamd Henry gedurende de Britse bezigheden in India (DigitalPersona, 1998b).

Het traditionele inkten van een vingerafdruk en het drukken ervan op papier is nog steeds een standaard, echter zijn er vandaag de dag ook electronische hulpmiddelen voor het verkrijgen van vingerafdrukken (Libov, 2001a).

De vraag is nu natuurlijk hoe dit process functioneerd, het antwoord op deze vraag wordt in bijlage 1.0 verschaft.

Het was Australië die in 1986 als eerste een nationaal computersysteem intregeerde voor het elctronisch implementeren en herkennen van vingerafdrukken (Libov, 2001a).

☜

Biometrie; Gezichtsherkenning

"… One must be careful to realize that computerized methods of [biometrical] recognition… do not recognize subjects in the same manner as a human brain."

Imagis 2004a

Veel verwarring is ontstaan betreffende dit onderwerp door verkeerde en/of misleidende informatie, welke is verstrekt door zowel verkopende organisaties als de media.

Mensen kunnen eenvoudig een gezicht herkennen, echter, wanneer een persoon voor lange tijd niet gezien is zijn wij vrijwel niet meer instaat om zijn of haar gezicht te herkennen. Een geautomatiseerd gezichtsherkenning systeem is hier wel toe instaat (Imagis, 2004g).

Wij vervolgen dit onderwerp in bijlage 1.1 In deze bijlage worden ook de False Rejection Rates en False Acceptance Rates behandeld.

Gezichtsherkenning systemen, Face-Recognition Systems (FRS), kunnen via wiskundige interpretaties van het gezicht bepaalde kenmerken vaststellen en vastleggen. Deze wiskundige berekeningen worden ook wel ‘encode strings’ genoemd. De encode strings vormen de basis voor de vergelijking, door middel van het toepassen van kunstmatige intelligentie is het FRS instaat om de encode strings te creëren en vervolgens te vergelijken (Imagis, 2004g).

☜

Biometrie; Irisherkenning

Irisscans onderscheiden zich door de distributie van kernmerken zoals de lengte, vezels, diepte, ringen, spikkels en donkere oppervlakken in het oog haar gekleurde slijmvlies. De scanning wordt gedaan met een infrarood licht welke een reflectie reduceert en door eventuele contactlenzen of bril heen dringt. Een irisscan is een minder vertrouwde techniek dan een retinascan, maar ondanks dat toch bijzonder wel functionerend onder verscheidene etnische groepen en daarbij is het ook nog eens extreem accuraat. The National Physical Lab in de UK heeft meer dan 2 miljoen monsters vergeleken zonder ook maar één verkeerde gelijke (DigitalPersona, 1998c).

Wij komen later, in onze Algemene Conclusie Betreffende: Biometrie, nog terug op irisscans.

Iris scans worden steeds vaker ingezet ter verificatie of als ondersteuning voor vingerafdrukken of gezichtsherkenningen (DigitalPersona, 1998c).

☜

Biometrie; Retinaherkenning

Retinascans richten zich op het bloedpatroon van de vezels in de retina, gelegen achterin het oog. De scan wordt uitgevoerd met een lage intensiteit van licht en is de meest accurate scan mogelijk. Echter is deze scan bijzonder moeilijk uit te voeren omdat de persoon voor enkele seconden dient te kijken naar een bepaald punt zonder knipperen met zijn/haar ogen en daardoor is het te gelimiteerd voor identificatie (Spinella, 2003a).

Biometrie; Hand-Geometrie

Bij handgeometrie worden de lichamelijke karakteristieken van de gebruikers hand en vingers gemeten in een 3D perspectief. Het is niet zo accuraat als de vingerafdruk en

daardoor minder geschikt als identificatie mogelijkheid (Williams, 2001a).

Biometrie; Spraak-Herkenning

Spraakherkenningstechnieken maken gebruik van de onderscheidbare kwaliteiten van een persoons zijn stem, sommige daarvan zijn gedragsgevoelig en andere fysiologisch. Spraakherkenning wordt veel toegepast in call-centers, thuisgevangenisapplicaties, banken, rekeningtoegang, etc. De stem wordt beschouwd als minder accuraat dan de vingerafdrukherkenning, irisherkenning en zelfs sommige vormen van gezichtsherkenning. Daarom wordt spraakherkenning niet als een geschikte identificatie mogelijkheid beschouwd (Myers, 2004a; Cherry, 2003b).

Biometrie; Handtekening Verificatie

Deze verificatie techniek werkt door middel van het herkennen van de manier waarop de gebruiker haar of zijn handtekening zet. De meetfactoren hangen af van de resultaten van onder meer de slag, lijnbeweging, snelheid en druk. Handtekeningen werden voor lange tijd gezien als een afdoende verificatietechniek, echter in onze huidige maatschappij is de vraag naar betere verificatietechnieken drastisch toegenomen en daarom behoort deze verificatietechniek vrijwel tot het verleden. Doch zal men deze techniek verder ontwikkelen om eventuele fraudeurs te kunnen opsporen, want voorloopig gebruiken we nog steeds handtekeningen ter verificatie (Cherry, 2003c; DigitalPersona, 1998d).

Biometrie; Andere soorten nog in onderzoek

Andere, meer exotische biometrische technieken, zijn nog in onderzoek. Deze andere biometrische technieken zijn: houding, reuk, het oor, vingergeometrie, bloedaderscans (*vanaf het eind van de pols tot het eind van de palm*) en het nagelbed welke wordt gebaseerd op de ribbels van de vingernagels. De houding is het tot nu toe meest bekende van deze biometrieën en is de laatste twee jaar openbaar gemaakt onder de naam “ID at a distance”. Deze campange koste meer dan 50 miljoen dollar en werd gesponsord door de US Department of Defence. Ongeveer 90% tot 95% werd correct geïdentificeerd aan de hand van de houding van de personen binnen een menigte. Daarom zou het mogelijk kunnen zijn dat deze technologie in de toekomst een

“… Ongeveer 90% tot 95% werd correct geïdentificeerd aan de hand van de houding van de personen binnen een menigte.”

belangrijk ‘anti-terreur’ identificatie middel zou kunnen worden (Cherry, 2003d).

Biometrie; en DNA?

Is DNA eigenlijk wel een biometrie? DNA is enigsinds wat anders dan de andere vormen van biometrie, laten we de hoofdzakelijke verschillen even op een rijtje zetten.

- Het vereist een tastbaar fysiek monster, niet gewoon een impressie of afbeelding;
- Het is niet een geautomatiseerd identificatie proces;
- Het is niet sjabloon gebaseerd en is eigenlijk een vergelijking van twee monsters.

Niettemin is het toch geclassificeerd als een biometrie welke tot een unieke identiteit zou kunnen dienen. Echter zitten er aan DNA zoveel aspecten vast dat zij nog lang niet zal kunnen dienen als identificatiemiddel (Stern, 2004h).

Biometrie en Standaardisatie

Indien men een succes wilt maken van het biometrisch paspoort dient men ondermeer te overwegen van welke standaard zij gebruik zal gaan maken. Hieronder hebben we de reeds bestaande standaarden uiteengezet.

- De BioAPI specificatie is ontwikkeld in samenwerking met meer dan 60 biometrie organisaties, en verschaft de mogelijkheid plug-in apparatuur met alle applicaties te kunnen laten samenwerken zonder dat het noodzakelijk is de bestaande applicatie te vervangen. BioAPI 1.1 was goedgekeurd bij het ANSI (*America National Standard Institute*) in februari 2002 en is nu onderdeel van het internationale standaardisatie proces.
- Het Common Biometric Exchange File Format, CBEFF, maakt het mogelijk om applicaties gebruik te laten maken van bestanden die biometrische informatie bevatten. Ook wordt er in het bestand de originele organisatienaam verwerkt en hun applicatienaam inclusief het versienummer.
- De XCBF standaard werd voorgesteld door de Oranization of the Advancement of Structured Infomation Standards ook wel het OASIS genoemd. Deze standaard moet het mogelijk maken om biometrische-files via het internet te versturen.
- Standaard uitwisselingsformaten zijn nog in ontwikkeling. Er is echter momenteel een vinger-minutiae standaard, onder de naam van AAMVA deze bevat ondermeer regelgevingen voor de

vingerafbeeldingen, en het formaat. Eveneens wordt er gewerkt aan de gezichts- en irisstandaarden die tot deze standaard zullen gaan behoren.

- Bijzondere industriële organisaties en associaties zijn ook bezig met de ontwikkeling van biometrische standaarden. De International Civil Aviation Organization (ICAO), een United Nation unit, adresseert de luchtvaart industrie voor het samenstellen van een logisch formaat wat moet dienen voor het opslaan van de biometrische data op een veilige en gecompliceerde manier. Eveneens zijn zij bezig met onderzoek naar het gebruik van diverse biometrie en de luchtvaart zal haar systemen op hun bevindingen aanpassen.

Conformiteit is echter een ander kwestie. Organisaties zijn bezig met het onderzoek naar en het ontwikkelen van onafhankelijker standaarden. Het Britse Common Criteria Certification programma definieert een Biometrics Protection Profile welke een standaard vormt voor de beveiliging van het biometrische identificatie systeem (Stern, 2004i).

Betrouwbaarheid en Accuratie

"Standard groups are addressing reliability issues by proposing common sets of tests and defined measurement criteria for biometric products. In addition, supporting hardware technology has advanced, so that a new generation of chips used in various biometric hardware devices has improved reliability" (Stern, 2004b).

Nieuwe en verbeterde technieken bieden de biometrische technologie een vooruitgang, mede hierdoor stijgt de betrouwbaarheid van biometrie. Het feit dat men zich nu bewust is dat kwalitatief goede monsters zorgdragen voor veel nauwkeurigere resultaten is niet in de laatste plaat belangrijk te noemen.

NIST gaf in mei 2003 vrij dat een combinatie van vingerafdrukken en gezicht de beste optie is voor de grenscontroles van de VS, later werd daar nog irisscans aantoegevoegd. "This blending of different types strengthens a security solution given the fact that no one biometric type is 100% accurate for a heterogeneous population" (Stern, 2004c).

> "… This blending of different types strengthens a security solution given the fact that no one biometric type is 100% accurate for a heterogeneous population."
>
> Stern 2004**c**

Biometrie en Wetgeving

"The governement has possession of a huge, ready-made facial image database - driver's license photos – and is looking into how they can be used. By law, the governement can't sell those photos to private companies, but there are no prohibitions on their use for surveillance purposes by the governement itself" (Blackburn, 2003b)

Het bovenstaande citaat illustreert precies het conflict tussen biometrie en wetgeving. Aan de ene kant zou het voor de efficiëntie van de biometrische identificatie het voordeligst zijn als zo veel mogelijk bedrijven en overheidsinstanties biometrische persoonsgegevens uitwisselen. Een (inter)nationale biometrie-database is een oplossing die in een klap alle identificatieproblemen zou oplossen. Hier komen wij later nog uitgebreid op terug.
Aan de andere kant vallen pasfoto's maar ook vingerafdrukken en irisscans onder de Wet bescherming persoonsgegevens en mogen ze dientengevolge niet door de overheid met bedrijven of door bedrijven onderling worden uitgewisseld zonder uitdrukkelijke toestemming van de eigenaar.

Dit betekent echter niet dat biometrische herkenning zijn efficiëntie verloren heeft. Bijvoorbeeld een bedrijf dat zijn productiewijzen en inboedel wil beschermen tegen diefstal en zijn personeel toegang biedt op basis van een irisscan heeft alleen van het betreffende personeel een irisscan nodig. Er hoeft dus niet noodzakelijkerwijs uitwisseling van gegevens plaats te vinden.

Wij denken dat voor de internationale uitwisseling van biometrische gegevens een wet moet komen met daarin een uitzonderingsclausule. Deze uitzonderingsclausule zal als functie hebben de uitwisseling van biometrische gegevens op internationaal gebied mogelijk te maken zodat de identiteitscontrolles aan grensen met een grotere efficiëntie kunnen worden uitegevoerd. Deze uitzondersclausule is noodzakkelijk ter voorkoming van conflicten met de Wet Bescherming Persoonsgegevens.

"… Identiteitsfraude is in Nederland een relatief onbekend begrip. Het komt hier veel minder voor dan bijvoorbeeld in de Verenigde Staten"

eJure 2004**a**

De Publiekelijke Acceptatie

Wij denken dat voor de invoering van het biometrisch paspoort men eerst het publiek van de noodzaak van het invoeren moet overtuigen.
Om het publiek te overtuigen moet men weten waar de angst voor de verandering zich bevindt, ofwel waarom het publiek

niet wil dat de betreffende verandering wordt doorgevoerd. Er zijn drie basis reden voor deze angst:

1. het doel van de verandering is niet bekend
2. men weet niet wat de verandering voor hem of haar persoonlijk inhoudt
3. men vindt de huidige situatie wel prima en heeft er geen enkel belang bij om deze te veranderen

(Droppler & Lauterburg, 1996a)

De oplossing van dit probleem is vrij eenvoudig samen te vatten, het doel van de invoer van het biometrisch paspoort, de concequenties en invloed die deze zal hebben en waarom de huidige situatie niet voldoet, zal moeten worden duidelijk gemaakt aan het publiek. Het is echter zo dat de uitvoer in de praktijk vaak niet zo simpel is (Droppler & Lauterburg, 1996a).

"Identiteitsfraude is in Nederland een relatief onbekend begrip. Het komt hier veel minder voor dan bijvoorbeeld in de Verenigde Staten" (eJure, 2004a). Echter, door de vergrote mogelijkheden, vooral via het internet, is dit probleem aan het verergeren. De lijdensweg van de slachtoffers is groot wegens een gebrek aan informatie wat te doen in degelijke situatie. "In Nederland zijn er nauwelijks gerechtelijke uitspraken bekend over digitale identiteitsdiefstal, noch is er specifieke op deze vorm van fraude gerichte wetgeving" (eJure, 2004b). Door de toename van dit probleem zullen de Nederlands, ofwel het publiek, het biometrisch paspoort waarschijnlijk makkelijker aanvaarden, immers het is voor hun eigen bescherming.

Opmerking: de kennis betreffende verandering is voornamelijk afkomstig van onze twee bronnen betreffende "change management".

Men zal willen weten wat biometrie precies is. De invloed die de invoer van het biometrisch paspoort heeft op individuën en hun privacy in het dagelijks leven dient te worden verstrekt aan het publiek.

Door deze stappen te ondernemen voorkomt de overheid een hoop problemen, goede voorlichting is een van de meest belangrijke elementen om een verandering succesvol doorgevoerd te krijgen.

Gevolgen van Biometrische Veranderingen

Een vaak over het hoofd geziene omstandigheid is dat door plastische chirurgie, ongelukken etc biometrische veranderingen kunnen optreden. Indien dit het geval is dan kan men zich dus afvragen of die persoon haar of zijn identiteit vervalt. Dit is een bijzonder gevoelig en discutabel

punt, echter wij denken dat de beste oplossing voor dit punt het volgende zou kunnen zijn: behalve de vinger- en gezichtsgegevens zal ook de irisgegevens een deel moeten kunnen uitmaken van het identiteit management systeem. Verder zou het noodzakelijk kunnen zijn om eveneens tandgegevens in dit systeem op te nemen, en misschien DNA-gegevens, echter wegens de verbonden kosten en moeizaamheden zal dit waarschijnlijk te veel complicaties met zich meebrengen om serieus overwogen te worden (Virgo, 2004).

De Algemene Conclusie Betreffende: Biometrie

Hoewel biometrie een zeer oude wetenschap is, is er pas de laatste paar jaren meer aandacht voor de massale toepassing ervan in identificatiemiddelen. Dat is te merken aan het aantal publicaties dat erover verschijnt en het aantal bedrijven dat zich met onderzoek naar biometrische identificatie bezigt.

Er zijn ruwweg zeven verschillende soorten biometrische identificatie, verschillend in het te herkennen lichaamsdeel en medium. Maar alle methoden hebben een paar kenmerken gemeen: bij allen berust de identificatie van een persoon op het vergelijken van gemeten waarden aan het lichaam van het persoon met waarden in een database.

De meest belangrijke biometrische technieken zijn vingerafdruk en gezichtsidentificatie. Irisscanning en retinascanning zijn identificatiemethoden die in de toekomst meer toegepast zullen worden.

Een discutabel punt binnen de biometrie is de veranderingen die mensen kunnen ondergaan in hun persoonlijke biometrische kenmerken. Plastische chirurgie, ongelukken en brandwonden kunnen leiden tot veranderde biometrische afmetingen, en daardoor een probleem vormen binnen het identificatiesysteem. Om dit af te vangen zou een irisscan onderdeel van het biometrisch paspoort moeten worden, gezien het feit dat de iris vrijwel nooit ernstige veranderingen ondergaat.

Om biometrische identificatie tot een succes te maken is het van belang om een standaard te hanteren om uitwisseling en vergelijking van materiaal mogelijk te maken. Verschillende bedrijven en organisaties houden zich bezig met de vraag welke standaard de beste oplossing zou zijn. Hierover is men het nog niet eens, maar wat wel vast staat is dat het combineren van verschillende technieken betrouwbaarder is dan het baseren van identificatie op één enkele methode. Een hindernis voor het algemeen invoeren van de biometrische herkenningsmethoden wordt gevormd door de Nederlandse wet bescherming persoonsgegevens. Deze wet verbiedt bedrijven het ongeoorloofd uitwisselen van persoonsgegevens, waar biometrische gegevens ook onder vallen.

Nederland is met de participatie in de ICAO al begonnen met de voorbereidingen voor het invoeren van het biometrisch paspoort. Voor de invoering van het biometrisch paspoort moet eerst de noodzaak hiervan aan het publiek duidelijk gemaakt worden, en uitgelegd worden wat biometrie exact inhoudt. Dit zal de acceptatie van het grote publiek vergroten.

Identiteit Management

Identiteit management is een erg wijd begrip, omdat we het toch zo goed mogelijk willen behandelen hebben we het meest vooraanstaande technologiebedrijf genomen wat op dit terrein actief is, genaamd Oracle. Echter, om een zo volledig mogelijk beeld te verschaffen geven wij nog een kort overzicht van andere belangrijke technologie bedrijven die actief zijn op het gebied van identiteit management.

- NEC
- RSA Security
- Generic
- Microsoft
- Novell
- Dell
- VeriSign
- And others

Door de jaren heen heeft Oracle haar veiligheidseisen voor hun databases en servers aangepast, echter met de laatste versie, de 10g versie; waar de ‘g’ staat voor “grid computing”, hebben ze de markt overtroffen. Onderzoek heeft uitgewezen dat de Oracle 10g databases en servers de meest geavanceerde en efficiënte systemen op de huidige markt zijn. Dit onderzoek is gedaan door de Edison Group, en op 25 mei werd dit onderzoek gepubliceerd. Naar eigen zeggen: “[…] Oracle is [now] recognized as the leading provider of secure infrastructure software with a record number of independent security evaluations” (Stern, 2004d).

> “[…] Oracle is [now] recognized as the leading provider of secure infrastructure software with a record number of independent security evaluations”
>
> Stern 2004**d**

Oracle

“Oracle partners with several vendors to supply biometric support because these vendors are expert in specific knowledge areas such as medical sciences and forensics that foster biometrics. Many biometric vendors already use the Oracle Database Server, mainly for storage purposes of temples and the images themselves. During the Oracle10g development cycle, Oracle worked with these vendors to fully exploit advanced database features to provide a more ‘biometrics-friendly’ solution” (Stern, 2004e).

En verder, het 10g pakket verschaft daarbij ook nog eens volledige ondersteuning voor het SSO systeem, Single Sign-On systeem, zijn er nog een aantal zaken die de 10g systemen ondersteunen, de hoofdzaken zijn:

- “Performance and scalability – searches involve looking at a very large numbers of candidates to

make a specific match – and this must be done in seconds."

- "Availability – searches occur continually and do not have a set "work-day" requiring 24x7 coverage"
- "Security – the data is sensitive, must be protected and should be tamper resistant" (Stern, 2004f).

Deze nieuwe technologie stelt de database instaat om te groeien tot maximaal 8 exabytes. Verder beschikt dit systeem over de capaciteit om twee vergelijkingen tegelijkertijd te behandelen. Bijvoorbeeld een vingerafdruk tegelijkertijd te vergelijken met een gezichtsafdruk en deze dan samen te brengen met de bijbehorende identiteit, en vervolgens een 'true' of 'false' match retour te zenden. De veiligheid van het systeem is uitermate belangrijk, immers alleen maar vertrouwde gegevens zullen in deze systemen worden opgenomen, de Data Guard zorgt ervoor dat er geen ongewenste bezoekers het systeem kunnen binnen treden, zoals hackers, verder verschaft het de mogelijkheid tot herstel van de database waardoor het systeem altijd beschikbaar is. Verder zijn RSA Security en Oracle samen bezig met de ontwikkeling van een waterdicht beveiligings systeem. Een vertraging bij de grens omdat het systeem gehackt is zou niet gepast zijn (RSA Security, 2004a-IAM; Stern, 2004j).

Dan zijn er nog de specifieke integraties die het Oracle platform als extra heeft toegevoegd voor het identiteit management system.

- Increased performance of identification searches;
- Flexibility and ease of use through SQL-queries across relational and biometric information;
- Easily extends to handle multi-modal biometrics;
- Reducing false non-match and false match rates thus improving accuracy and reliability;
- Providing another means of enrolment, verification, and identification if sufficient data cannot acquired from a given biometric sample;
- Adding a greater degree of security because it is more difficult to "spoof" a multimode biometric system. (Stern, 2004g)

Smartcards

Smartcards zijn kleine apparaten die zijn voor zien van een ingebouwde microprocessor welke als functie heeft gegevens

op te slaan en de mogelijkheid tot verwerking van deze opgeslagen gegevens verschaft.

Er zijn een aantal vormen van smartcards op de markt, we behandelen hen in het kort met informatie verkregen van de RSA Security.

De Stored Value Card is een opslag kaart met vastgelegde gegevens, deze kaart beschikt niet over een intelligente eenheid waardoor hij weinig verschilt van een opslag disk.

De Mircroprocessor Memory Cards, deze kaart bevat eigenlijk een geheel intern besturingssysteem en een RAM, Random Access Memory, voor tijdelijke opslag. Het EEPROM, Electronically Erasable Programmable Read Only Memory, bied volledige functionaliteit. Deze kaarten zijn complex en kunnen data verwerken op de kaart zelf maar niet zonder een daarvoor speciale hardware device.

Een smartcard als paspoort, licht makkelijk, efficiënt en veilig. Een droom die te mooi is om waar te zijn?

De Cryptografie Card, is vergelijkbaar met de MMC maar heeft daarbij nog eens de extra functie van encryptie van data. Deze kaart is “virtually ‘hacker-resistant’” en daarvoor uitermate geschikt als paspoort.

Bovendien is het niet noodzakkelijk dat de smartcard persoonlijke gegevens bevat, slechts een ‘sleutel’ voor het systeem om de bijbehorende identiteit te controleren in combinatie met die persoon zijn biometrische kenmerken is voldoende. Indien deze biometrische kenmerken van de desbetreffende persoon overeenkomen met gegevens in de database zal een positieve match worden geretourneerd. De sleutel is als het ware een directe link naar de persoonlijke gegevens van de betreffende persoon. De sleutel zal alleen in samenwerking met de juiste biometrische gegevens leiden tot een complete link (RSA Security, 2001a).

Security and Privacy

Government Technology Magazine’s Tech Trends 2002 publiceerde onlangs een MIT onderzoek waar wij de volgende regel in aan troffen: “the average machine is connected to the Internet for less than five minutes before an automated attack program scans it ... Once a system is compromised, it can be used as a jumping-off point for deeper attacks, as into (government) infrastructure and connected systems.” Het is dus van bijzonder belang dat het identiteit management system niet alleen bijzonder goed en geavanceerd beveiligd is maar ook nog een op een apart

netwerk moet staan, men zou dus een speciaal intranet moeten ontwikkelen om de gegevens via hoge encryptie, 1024bit bijvoorbeeld, te verzenden naar het systeem wat om de gegevens vraagt.

Een ander aspect is de Identiteit Management Systems's manager. Deze persoon, of waarschijnlijk personen, beschikken over enorm veel macht, daarom zal hun macht gedeeld moeten worden en zover mogelijk verminderd moeten worden. Het systeem moet eigenlijk op zichzelf kunnen functioneren.

Voor meer informatie verwijs ik door naar bijlage 2.0 User Management of the Identity Management System.

☜

Het Verwerken van Biometrische Gegevens in een Biometrisch Paspoort

Nu wij de meest belangrijke details betreffende identiteit management, smartcards en natuurlijk biometrie zelve behandeld hebben leek het ons mogelijk om de vraag te antwoorden betreffende hoe deze gegevens dan op te nemen in een paspoort.

Het huidige paspoort is een klein boekje gemaakt van speciaal papier; het toekomstige paspoort zal er echter veel meer uit gaan zien als een bankpasje. De Cryptografie Card zal het nieuwe paspoort gaan worden, maar zal geen persoonlijke gevens bevatten slechts een versleutelde link die de sleutel vormt voor het identiteit management systeem naar de gegevens van de betreffende persoon. Doordat het nieuwe biometrisch paspoort geen zichtbare gevens bevat, en zij alleen via een combinatie van vingerafdruk-, gezichtsherkenning en de smartcard gelezen kan worden, zal de veiligheid toenemen.

Future aspects

Wij verwachten dat bepaalde risico's verbonden zijn aan de invoer van een geheel automatisch identificatie systeem, eveneens verwachten wij dat zullen de kosten erg hoog zullen zijn. Toch verwachten we dat als de overheid samen werkt met het bedrijfswezen en dit een effectieve oplossingen kan bieden voor zowel het bedrijfswezen als de overheid. Wij denken namelijk dat de overheid, tegen betaling, organisaties een totaal pakket zou kunnen aanbieden. Dit totaal pakket dient niet alleen te voldoen aan de wetgevingen omtrend persoons bescherming, maar zal ook veilig moeten zijn.

Wij stellen ons dan ook het volgende voor:

De overheid introduceert in samenwerking met Oracle, NEC, RSA Security, aCG en eventuele andere partijen een goed biometrisch identificatie systeem, welke betrouwbaar, veilig, en stabiel is. Vervolgens heeft de overheid de macht om haar burgers de verplichting op te leggen de benodigde biometrische gegevens af te staan en een nieuw paspoort in te voeren, een smartcardpaspoort. Een vingerafdruk, gezichtsafdruk en een irisafdruk zullen benodigd zijn voor een solide systeem en werking van het systeem met back-up functie. Normale identificatie vindt plaat door een combinatie van vinger en gezicht herkenning echter indien er twijfel is of door een bijzonder aspect dit onmogelijk is kan men altijd terug vallen op de irisherkenning. Wanneer dit allemaal gedaan en ontwikkeld is kan de overheid het bedrijfswezen de mogelijkheid bieden om hun werknemers en cliënten te laten identificeren met behulp van een speciaal daarvoor ontwikkeld systeem, welke gelijk daarmee de standaard zal gaan vormen. Let wel, dat er nadrukkelijk geen persoonsgegevens worden uitgewisseld tussen overheid en bedrijf, slechts een sleutel (het smartcardpaspoort) en gegeven (verkregen via een scanmodule) worden gecontroleerd en vervolgens wordt er een match of non-match retour gezonden naar het bedrijf. Naar onze verwachting zullen de gemaakte kosten voor een bijzonder groot deel terug te verdienen zijn alleen al aan minder kosten van identiteitsdiefstal, fraude en een verminderende hoeveelheid administratiekosten. Dit gezien het feit dat Business Intelligence (BI) de hoogste ROI (Return on Investment) heeft van alle ICT toepassingen, al volgens de Gartner Group. Daarbij zal als bonus het bedrijfswezen dan nog eens een extra deel kunnen terug vorderen waardoor de implementatie van het biometrisch paspoort een succes zou kunnen worden.

Conclusie

De hoofdvraag

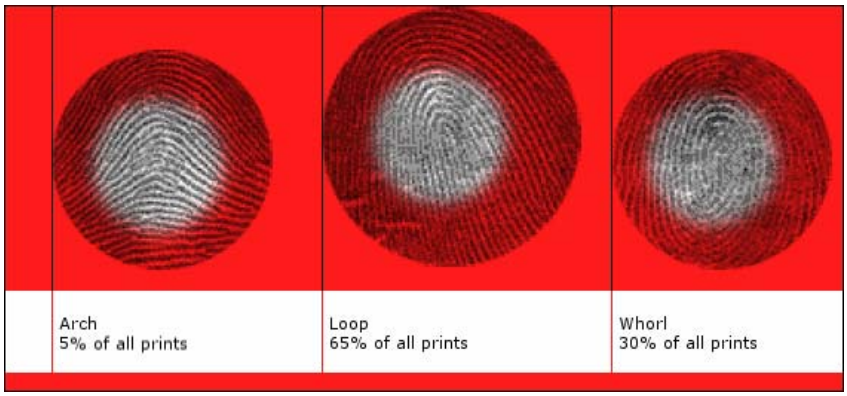
“In hoeverre kunnen we de identiteit managen met behulp van de unieke menselijke kenmerken verstrekt door een biometrisch paspoort?”

Het antwoord

Het biometrisch paspoort biedt veel nieuwe mogelijkheden voor identificatie en verificatie. Met behulp van biometrische technologieën; vingerafdrukken, irisscans en gezichtsherkenning, en nieuwe technieken zoals de crypto-smartcards en krachtige databases is er een mogelijkheid ontstaan tot een bijna perfecte oplossing voor het management van identiteiten. Anderzijds is het de vraag of het publiek het biometrisch paspoort wilt accepteren omdat het mogelijk is dat het publiek de invoer van het biometrisch paspoort ziet als een inbreuk op hun privacy. Om deze rede is een goede voorlichting omtrent de invoering van het biometrisch paspoort noodzakelijk.

Bijlage 1.0 — Vingerafdrukken

Vingerafrukherkenningsapparatuur scant het unieke patroon van lijnen van de vingertop. Deze unieke patronen kunnen in drie vormen voorkomen, de lus, buigingen en de spiraal vorm, zie afbeelding 1.0

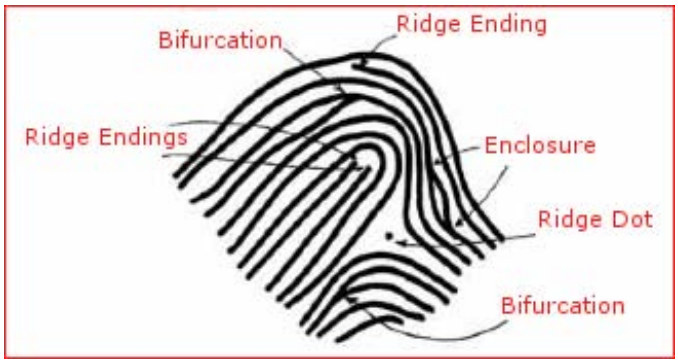


Afbeelding 1.0

De lus vorm is van toepassing op wel 65% van alle vingerafdrukken, een ‘whorl’ 30% en een buiging 5%. Het detecteren van een lus gebeurt door het nemen van de start van de ribbel-lijn tot het middelpunt en dan ‘loop-back’. Een whorl kan worden gedetecteerd door het nemen van het begin van een concentretische circel naar het centrum van de afdruk. De whorl can worden gedetecteerd door het nemen van het begin van de ‘whorl-vorm’. Dan de laaste, de buiging welke start aan een kant en vervolgens doorloopt naar de andere kant van een vinger.

Er zijn diverse methoden die het indentificeren mogelijk maken van iemands afdruk. De meest bekende methode gaat om het herkenning en vergelijken van de “minutiae” punten van de vingerafdruk. De “minutiae” punten zijn de punten waar de afdruk ribbels samen komen en eindigen. “Minutiae” punten kunnen worden overwogen als het *unieke* van een vingerafdruk. De scanners maken gebruik van de X en Y technologie, de “minutiae” punten zijn niet anders dan de plaats bepalingen voor de X en Y waarden.

In afbeelding 1.1. worden de eigenschappen van de “minutiae punten” afbeeld en in tabel 1.1. worden de eigenschappen uiteengezet.



Afbeelding 1.1

Bifurcation (*zich-afsplitsen*)	Het punt waar de ribbel splijt in meerdere ribbels, de zogehete 'takken'.
Divergence (*afwijking*)	Dit is het punt waar de paralle ribbels of splijten of samen komen.
Enclosure-occurs (*aanvullen*)	Wanneer een ribbel splijt in twee takken en later weer samen komt heet dit een 'enclosure'.
Ending-occurs (*beëindigen*)	wanneer ribbels eindigen
Valley-spaces (*kloven*)	Deze bevinden zich aan beide kanten van een ribbel en worden ook wel kloven genoemd.

Tabel 1.1

Het is gebruikelijk dat wanneer een vinger wordt gescand er tussen de 30 en 40 "munitiae" punten worden gedetecteerd. Volgens de FBI (Federal Bureau of Investication) worden maximaal slechts 8 gelijke "munitiae" punten kunnen gedeeld door twee individuën.

Een andere methode om een persoon te indentificeren aan de hand van een vingerafdruk is door het 'tellen' van de ribbels tussen de punten, dit is mogelijk door het nemen van de verschillen geproduceerd door ultra-sound-waves. Deze vorm is gebaseerd op patronen en vraagt enorm veel rekencapaciteit van de processor en is daarom minder gebruikt. Wel is deze vorm moeilijker te vervalsen en buitegewoon betrouwbaar. De eerste methode die we hebben behandeld heeft namelijk als nadeel dat niet iedere huid even goed is voor het vinden van "munitiea-points". Een combinatie van deze twee is vrijwel de beste oplossing.

We kunnen nog veel meer over het digitaliseren van een vingerafdruk vermelden alleen leek dat ons niet noodzakelijk. In de volgende sectie zullen we de gezicht-kenmerken behandelen, vervolgens zullen we nog een andere biometrische oplossing, het iris-scanning, behandelen. Verder zullen we kort nog een paar andere biometrische vormen behandelen om een volledig beeld te geven.

Bijlage 1.0 is tot stand gekomen met behulp van:
Libov, paginas: 1-4
Marchant, paginas: 1-3

Bijlage 1.1 — Gezichtsherkenning

In onze imperfecte wereld is het maar de vraag of het beeldbestand dat we krijgen aangeleverd, zoals gescande pasport foto's, inderdaad kwalitatief genoeg zal zijn voor het FRS. Imagis zegt er het volgende over: "Despite these varying contexts, users still expect a high rate of match success with probe images. As these expectations are extremely difficult to live up to, projects are sometimes labelled as failures despite producing advantageous results and obvious benefits."
Overigens blijft het daar niet bij volgens Imagis; "An equall common expectation is that surveillance footage of atrocious quality is good fodder for FRS. While image enhancement and manual intervention in the encode process may assist with FR matching, if the data involves low quality or highly disparate imagery, the results will be unpredictable and modest at best."

"All biometric technologies perform better with good quality data and with consistency between the enrolled data and the probe data"

Imagis 2004**b**

Daarbij komt dat FRS niet goed overweg kan gaan met veranderingen die mensen krijgen dan wel aanbrengen in het gezicht. Een van de meest voorkomende veranderingen wordt veroorzaakt door de plastische chirurgie. Dit brengt ons vervolgens naar de FAR en FRR, False Acceptance Rates and False Rejection Rates.

"When someone asks, 'What is your system's FRR/FAR?' they are not taking into account that the numbers are only meaningful in the context of a specific set of data…"

Imagis 2004**c**

Biometrie; FAR and FRR
Deze ratio worden meestal gebruikt ter identificatie van de systeem capaciteit. De FAR en FRR geven het aantal verkeerde en negatieve en positieve gelijke aan, gedurende de biometrische evaluatie en verificatie.

Verificatie is principieel gezien de determinatie van 'bent u daadwerkelijk degene die u claimt te zijn?'. Let wel dan identificatie een proces is van 'wie u zou kunnen zijn', deze dienen niet verward te worden.

Vervolgens is het ons doen om FR te gebruiken ter identificatie en zodoende moeten we het eigenlijk niet hebben over de FRR en FAR maar over de CMC (*Cumulative Match Characteristis*).

Biometrie; CMC
CMC is het percentage hoe vaak een afbeelding overeenkomt met een afbeeldingdatabase. Vervolgens zou het resultaat moeten luiden: 'most-likely image'.

Met andere woorden, als een persoon terecht en correct is geïdentificeerd door de algoritmes die zijn los gelaten op de database, beschrijft CMC de waarschijnlijkheidsgraad dat de gelijke naar voren komt in de eerste 1, 2, 3 etc. positie. Vervolgens zal er met een percentage aan worden gegeven hoeveel de afbeelding gelijk is aan de ingevoerde afbeelding.

Ter illustratie verstrekken wij een voorbeeld-scenario:

Gezichtsherkenning:
Een meisje met veel make-up, slechte belichting en een lage resolutie foto dient te worden geïdentificeerd. Dit bestand wordt vervolgens gevonden met een rating van 0.9249 en dat is in dit geval de 20ste plaats. Dit is natuurlijk nog steeds een behoorlijke waarde, doch illustreert dit maar al te duidelijk hoe beperkte informatie het herkenningsproces beïnvloed. Database design heeft daarbij nog eens de beperking van het fenomeen ‘garbage in, garbage out’.

Bijlage 1.1 is tot stand gekomen met behulp van:
Williams, paginas: 5-7
Imagis, paginas: 2-10

Bijlage 2.0 — Bronbeoordeling

1. **O'Neill, M.** (2001). Concise Dictionary & Thesaurus.
   Edinburgh: Chambers Harrap Publishers Ltd.

   Een woordenboek dient informatie te verstrekken die betrouwbaar is; een woordenboek wordt om die reden eerst bijzonder grondig nagekeken op fouten, incorrectheden en onduidelijkheden alvorens zij wordt gepubliseerd. Deze grondigheid garandeerd een goede informatie voorziening.

2. **Myers, L.** (2004, April 19). An Exploration of Voice Biometrics.
   Retrieved September 18, 2004 from the World Wide Web:
   http://www.sans.org/rr/papers/6/1436.pdf

   SANS is werelds meest vertrouwde bron voor informatie betreffende: beveiliging training and certificatie. SANS is opgericht in 1989 en kwam in 1991 met het GIAC-certificaat. Al de schrijvers zijn grondig getoets en beschikken een GIAC-certificaat. Dit certificaat betekent dat men instaat is grondig onderzoek te verrichten en ook daad werkelijk kennis heeft van het betreffende onderwerp, zowel in de praktijk als op papier. De Gartner Group, welke is "the leading provider of research and analysis on the global IT intrustry" (Gartner, *http://www4.gartner.com/5_about/company_information/41a.html*), heeft het GIAC-certificaat grondig gecontroleerd en onderzocht, en kwamen tot de conclusie dat dit certificaat voldeed aan de gestelde eisen. (Garter Research: GIAC "the preferred credential")

   Meer informatie betreffende een van boven genoemde organizaties kunt u op de volgende sites vinden:
   - http://www.sans.org
   - http://www.giac.org
   - http://www.gartner.com

   Bij deze persoon staat explicit vermeld dat de betreffende persoon een GIAC Certificaat bezit, verder is duidelijk aan de document strucutuur te zien dat deze persoon een wetenschappelijke opleiding genoten heeft en weet hoe documentatie op te stellen.

3. **Cherry, K.** (2003, November). Biometrics: An In Depth Examination.
   Retrieved September 18, 2004 from the World Wide Web:
   http://www.sans.org/rr/papers/6/1329.pdf
   zie punt 2

4. **Soutar, C., & Roberge, D., & Stoianov, A., & Gilroy, R., & Kumar, V. B.V.K.** (undefined)
Biometric Encryption™.
Retrieved September 16, 2004 from the World Wide Web:
http://bioscrypt.com/assets/Biometric_Encryption.pdf

De heren zijn werkzaam in dit vakgebied bij Mytec Technologies Inc, de heer Roberge werkt bij Forensic Technologies Inc, een extern bedrijf en de heer Kumar zit bij “The Department of Elecritical and Computer Engineering, Carnegie Mellon University” Verder is de volgende quote van belang, “The content of this article appears as chapter 22 in ICSA Guide to Cryptograhy, edited by Randall K. Nochols, McGraw-Hill (1999)” Soutar, Colin; Roberge, Danny; Stoianov, Alex; Gilroy, Rene and Kumar, Vijaya B.V.K., page 1. Het is duidelijk dat deze personen weten waar zij over schrijven en dat is ook goed te zien aan de opmaak van het document.

5. **Greenwood, D.** (2002, December 04). Identity Management.
Retrieved September 16, 2004 from the World Wide Web:
http://www.ec3.org/Downloads/2002/id_management.pdf

Dit document is niet geschreven door alleen de heer Greenwood, Greenwood is de “director” van de NECCC, National Electronic Commere Cooridnating Council, en in samenwerking met vele personeelsleden is dit document tot stand gekomen. Velen hebben een hoge wetenschappelijke opleiding genoten, zoals MIT. Verder zijn er bijlagen toegevoegd die de controlle van het document en haar informatie vergemakkelijken en eveneens hier is de opmaak van het document bijzonder netjes.

Bijlage 3.0 — Bibliografie

Blackburn, D. (2003, April 07). Face Recognition 101: *A Brief Primer.*
Retrieved October 01, 2004 from the World Wide Web:
http://www.frvt.org/DLs/FR101.pdf

Parenthetical notes
(Blackburn, 2003**a**, **p.1**)
(Blackburn, 2003**b**, **p.2**)

Cherry, K. (2003, November). Biometrics: An In Depth Examination.
Retrieved September 18, 2004 from the World Wide Web:
http://www.sans.org/rr/papers/6/1329.pdf

Parenthetical notes
(Cherry, 2003**a**, **p.1**)
(Cherry, 2003**b**, **p.11**)
(Cherry, 2003**c**, **p.11**)
(Cherry, 2003**d**, **p.12-13**)

College Bescherming Persoonsgegevens. (January 2002). Mag het een bitje minder zijn?
Sdu Grafisch Bedrijf

DigitalPersona™. (1998). Biometric Solutions to Personal Identification
Retrieved September 18, 2004 from the World Wide Web:
http://www.digitalpersona.com

Parenthetical notes
(DigitalPersona, 1998**a**, **p.3**)
(DigitalPersona, 1998**b**, **p.2-3**)
(DigitalPersona, 1998**c**, **p.6**)
(DigitalPersona, 1998**d**, **p.8**)

Doppler, K., & Lauterburg, C. (1996). Change Management.
Nederland: Addison-Wesley

Parenthetical notes
(Doppler & Lauterburg, 1996**a**, **p.22-40**)

eJure. (April 24, 2004). Identiteitsfraude in Nederland.
Retrieved October 10, 2004 from the World Wide Web:
http://www.ejure.nl/articles/dossier_id=17/id=37/show.html

Parenthetical notes
(eJure, 2004**a**, **p.1**)
(eJure, 2004**b**, **p.1**)

Edison Group Inc (2004, May 25). Comparative Managemetn Cost Study Oracle Database10g and Microsoft SQL Server 2000.

Federal Reserve Bank of Boston, (2001). Identity Theft.
Retrieved September 16, 2004 from the World Wide Web:
http://bos.frb.org/consumer/idenity/idtheft.pdf

Graaf, de T. (December 19, 2004). Biometrie in Reisdocumenten.
Retrieved October 05, 2004 from the World Wide Web:
http://www.minbzk.nl/contents/pages/1010/brief_tk_biometrieinreisdocumenten.pdf

Greenwood, D. (2002, December 04). Identity Management.
Retrieved September 16, 2004 from the World Wide Web:
http://www.ec3.org/Downloads/2002/id_management.pdf

Greuter, R. (October, 2004). Clientless Secure Remote Access. Infosecurity.nl, 5, 41-45

Gupta, M. (2001, March 16). Biometric Technologies Overview.
Retrieved September 17, 2004 from the World Wide Web:
http://www.giac.org/practical/gsec/Manoj_Gupta_GSEC.pdf

Hairston, M., Ruszkiewicz, J., Friend, C. (1999). The Scott, Foresman Handbook for Writers.
New-York: Addison Wesley Longman Inc.

Have, ten Steven & Wouter. (2004). Het Boek Verandering.
Amsterdam: Nieuwezijds.

Hes, R., & Hooghiemstra, T.F.M., & Borking, J.J. (September, 1999). At face value:
On biometrical identification and privacy
Retrieved October 06, 2004 from the World Wide Web:
http://www.cbpweb.nl/downloads_av/AV15.pdf

Houghton Mifflin Company (2003). The American Hertiage Dictionary of the English Language.
Houghton Miffling; *Fourth Edition*
Accessed by GuruNet Membership.

Imagis Technologies Inc (2004). Face Value.
Retrieved September 16, 2004 from the World Wide Web:
http://www.imagistechnologies.com/files/PDF/Imagis_White_Paper_-_Face_Value_-_Successful_FR_Implementations.pdf

Parenthetical notes
(Imagis, 2004**a**, **p.2**)
(Imagis, 2004**b**, **p.6**)
(Imagis, 2004**c**, **p.7**)
(Imagis, 2004**d**, **p.15**)
(Imagis, 2004**e**, **p.16**)
(Imagis, 2004**f**, **p.17**)
(Imagis, 2004**i**, **p.2-5**)

LaBriola, B., & Boly, J. (2002). RSA SecurID: Providing Identity, Establishing Trust, Enabling e-Business.
RSA Security Inc.

Libov, Y. (2001, July 09). Biometrics: Technology that gives you a password you can't share.
Retrieved September 18, 2004 from the World Wide Web:
http://www.sans.org/rr/papers/6/99.pdf

Parenthetical notes
(Libov, 2001**a**, **p.2-3**)

Marchant, Z. (2001, January 19). Biometrics: Fingerprint Authentication.
Retrieved September 17, 2004 from the World Wide Web:
http://www.giac.org/practical/gsec/Zeena_Merchant_GSEC.pdf

Martinello, P., & Macolina, D., & Dworkin, D. (2003). RSA ClearTrust Web Access Management.
RSA Security Inc.

Myers, L. (2004, April 19). An Exploration of Voice Biometrics.
Retrieved September 18, 2004 from the World Wide Web:
http://www.sans.org/rr/papers/6/1436.pdf
Parenthetical notes
(Myers, 2004**a**, **p.4-8**)

NEC (UK) Ltd; Security Solutions; Business Solutions Division (July 2004). NEC's Advanced Digital Identity Solutions: Overview.
Retrieved September 25, 2004 from the World Wide Web:
http://www.nec.co.uk/adis_white_paper.aspx

O'Neill, M. (2001). Concise Dictionary & Thesaurus.
Edinburgh: Chambers Harrap Publishers Ltd.

Ravestein, & Zwart. (August 31, 2004). Gemeenten Testen Biometrisch Paspoort.
Retrieved October 05, 2004 from the World Wide Web:
http://www.zibb.nl/overheid/zoekinzibbdetail.asp?portalnaam=overheid&artnr=811189&artsrtnr=730&knooppunt=216

Ravestein, & Zwart. (October 5, 2004). Misbruik Paspoort Neemt Toe.
Retrieved October 05, 2004 from the World Wide Web:
http://www.zibb.nl/overheid/nieuwsbericht.asp?artnr=827881&versie=1
Parenthetical notes
(Ravestein, & Zwart, 2004**a**, **p.1**)

Rein, van, R. (October, 2004). De Kraakbaarheid van Windows Passwords. Infosecurity.nl, 5, 29-32

RSA Security®. (2004). Identity & Access Management.
RSA Security Inc.
Parenthetical notes
(RSA Security, 2004**a-IAM**, **p.2-3**)

RSA Security®. (2004). RSA Sign-On Manager.
RSA Security Inc.

RSA Security®. (2001). The Cryptographic Smart Card
RSA Security Inc.
Parenthetical notes
(RSA Security, 2001**a**, **p.1-6**)

Spinella, E, (2003, May 28). Biometric Scanning Technologies: Finger, Facial and Retinal Scanning.
Retrieved September 16, 2004 from the World Wide Web:
http://www.giac.org/practical/GSEC/Edmun_Spinella_GSEC.pdf

Soutar, C., & Roberge, D., & Stoianov, A., & Gilroy, R., & Kumar, V. B.V.K. (undefined)
Biometric Encryption™.
Retrieved September 16, 2004 from the World Wide Web:
http://bioscrypt.com/assets/Biometric_Encryption.pdf

Stern, S.A. (2004, January). Oracle and Biometrics.
Oracle Corporation; World Headquarters, Redwood Shores.

Parenthetical notes
(Stern, 2004**a**, **p.7**)
(Stern, 2004**b**, **p.9**)
(Stern, 2004**c**, **p.9**)
(Stern, 2004**d**, **p.11**)
(Stern, 2004**e**, **p.12**)
(Stern, 2004**f**, **p.13**)
(Stern, 2004**g**, **p.14**)
(Stern, 2004**h**, **p.5**)
(Stern, 2004**i**, **p.6-7**)
(Stern, 2004**j**, **p.13**)

Terstegge, J.H.J. (July 6, 2000). Web Bescherming Persoonsgegevens.
Retrieved October 05, 2004 from the World Wide Web:
http://home.planet.nl/~privacy1/wbp.htm

Virgo, P. (July 2004). Legislation on Identity Cards Response by the Institute for the Management of Information Systems to the Home Office Consultation.
Retrieved October 01, 2004 from the World Wide Web:
http://www.imis.org.uk/40_info_source/10_news/ID_cards_EURIM

Wayne, P. (2003, February 06). Biometrics: A Double Edged Sword – Security and Privacy.
Retrieved September 18, 2004 from the World Wide Web:
http://www.sans.org/rr/papers/6/137.pdf

WebOpedia (2004).
Retrieved September 16, 2004 from the World Wide Web:
http://www.webopedia.com/

Parenthetical notes
Verification: http://www.webopedia.com/TERM/verification.html
Authentication: http://www.webopedia.com/TERM/authentication.html
Identification: http://www.webopedia.com/TERM/identification.html

Williams, G. (2001, December 24). More than a pretty face, Biometrics and SmartCard Tokens.
Retrieved September 18, 2004 from the World Wide Web:
http://www.sans.org/rr/papers/6/125.pdf

Parenthetical notes
(Williams, 2001**a**, **p.7**)

Winter, de, B. (October, 2004). Bomb on Board! Beveiliging of Privacy. NetOpus 7 11

Wittich, P. A. (2003, April 21). Biometrics: Are YOU the Key to Security?
Retrieved September 18, 2004 from the World Wide Web:
http://www.sans.org/rr/papers/6/850.pdf

Zimmerman, M. (2002, February 06). Biometrics and User Authentication.
Retrieved September 18, 2004 from the World Wide Web:
http://www.sans.org/rr/papers/6/122.pdf