Notitie

gemmissaal
14/10/99

Aan Minister van Boxtel	Afdeling
Van DGOB	Afdeling DGOB
Doorkiesnummer (070)	Kamer
Gesteld door	Doorkiesnummer (070)
Via	Afdeling
Iaa	Afdeling
Kenmerk NGR99/N87211	Datum 1 oktober 1999

Onderwerp
Aanbieding rapport Biometrie door Registratiekamer op 5 oktober 11.30 uur

Inleiding
Op 5 oktober 1999 zal de Registratiekamer u het (Engelstalige) rapport over biometrische identificatie ("At face value, on biometrical identification and privacy") aanbieden.
De plechtigheid vindt plaats in Nieuwspoort (Van der Poelzaal) om 11.30 uur.

Onderstaand wordt het programma nader toegelicht, de samenvatting van het rapport weergegeven en de reactie van BZK daarop, mede in het licht van de Nieuwe Generatie Reisdocumenten.
Bijgevoegd treft u een spreektekst aan die u kunt uitspreken bij overhandiging van het rapport.

Programma
Voorafgaand aan de aanbieding van het rapport zullen respectievelijk (John) Borking, plv. voorzitter, en (Peter) Hustinx, voorzitter, een inleiding verzorgen.
Borking zal in zijn inleiding met betrekking tot de techniek van biometrische identificatie de volgende vragen beantwoorden:
- wat is biometrie en biometrische identificatie
- waarom is het van belang
- methoden en technieken
- is er een privacy probleem

Hierna zal Hustinx ingaan op het juridisch kader en antwoorden geven op de navolgende vragen:
- biometrische gegevens zijn bij uitstek geschikt voor identificatie, maar wat zegt de wet
- zijn biometrische gegevens persoonsgegevens
- welke voorwaarden gelden voor het verantwoord gebruik van biometrische gegevens:
  - zijn de biometrische gegevens nodig
  - zijn de gegevens rechtmatig verkregen
  - is er sprake van 'bijzondere gegevens' zoals medische gegevens
  - zijn de gegevens voldoende beveiligd

- rechtvaardigt het doel eventuele centrale opslag van biometrische gegevens

Aldus geeft de Registratiekamer de voorzet voor een discussie met u over het gebruik van biometrische gegevens in het paspoort. Vraag die de Registratiekamer daarbij stelt is: rechtvaardigt het doel de centrale opslag van gegevens?
De Registratiekamer is van mening dat een goed beveiligd paspoort natuurlijk een gerechtvaardigd belang is, maar hoe zit het met de opslag en de beveiliging van de gegevens? En hoe worden de gegevens verkregen? Door middel van een wettelijke verplichting? Zie ook bijgevoegd persbericht van de Registratiekamer.

Vervolgens wordt u het rapport aangeboden en u in de gelegenheid gesteld te reageren op de inleidingen van beide heren.
Uw reactie zou met name in moeten gaan op de betekenis van biometrie voor zowel het paspoort als voor de elektronische identiteitskaart en uw zienswijze op de voorwaarden waaronder biometrie voor dit doel kan worden toegepast. Inhoudelijk ingaan op het rapport is op dit moment nog niet aan de orde. Zie ook bijgevoegde spreektekst.

Directie Voorlichting ([redacted]) is geïnformeerd en onderhoudt kontakt met zijn collega van de Registratiekamer.
Van NGR zal in ieder geval [redacted] aanwezig zijn.

Samenvatting rapport Biometrische Identificatie
Het rapport Biometrische Identificatie (nederlandse titel van het engelstalige rapport 'At face value, on biometrical identification and privacy') is opgesteld door de Regisratiekamer (de heren Borking, Hes en Hooghiemstra) met bijdragen van TNO.

Het rapport geeft een uiteenzetting van de technische en juridische aspecten van biometrie en gaat in op de noodzakelijke privacywaarborgen.

De hoofdlijn van de bevindingen luiden als volgt:
De exclusiviteit van gegevens is binnen de informatiebeveiliging een belangrijk kwaliteitsaspect. Om onbevoegden buiten te kunnen sluiten is het controleren van de toegang tot informatie cruciaal. Daarvoor is identificatie (wat is de identiteit van de persoon) en authenticatie (kan deze identiteit bevestigd worden door vergelijking met een ander betrouwbaar gegeven) nodig.
Het rapport stelt vast dat het gebruik van biometrie de kwaliteit van de identificatie en authenticatie kan verhogen. Lichaamskenmerken zijn immers nagenoeg uniek en niet overdraagbaar aan derden.
De noodzaak om het gebruik van biometrie te overwegen komt voort uit de constatering dat huidige vormen van identificatie en authenticatie -zeker in situaties waarbij handelingen en transacties op afstand, met gebruikmaking van computers en netwerken, plaatsvinden- niet volledig persoonsgebonden zijn en dus fraudegevoelig.

Biometrische kenmerken kunnen gebaseerd zijn op persoonskenmerken en op gedragskenmerken. De meest geavanceerde toepassingen hebben betrekking op persoonskenmerken, zoals vingerafdruk, netvlies en iris, gezichtsvorm, hand- en vingergeometrie.

Kern van het rapport is de privacy-aspecten van het gebruik van biometrie. Verantwoorde inzet van biometrische identificatie betekent dat rekening wordt gehouden met de wetgeving voor de bescherming van persoonsgegevens. In dit verband wordt gerefereerd aan de Europese privacyrichtlijn en (straks) de Wet bescherming persoonsgegevens. De vragen die daarbij van belang zijn, zijn:

- welke gegevens zijn echt nodig voor het doel?
- worden de gegevens rechtmatig ingewonnen; is de betrokken persoon geïnformeerd?
- is er sprake van 'bijzondere gegevens' (dit zijn gegevens over iemands ras of gezondheid; verwerking van bijzondere gegevens is in beginsel verboden)?
- zijn de biometrische gegevens zo opgeslagen dat ze niet meer terug te voeren zijn tot de oorspronkelijke gegevens?
- is het mogelijk om de meting van de gegevens en de verificatie decentraal te laten plaatsvinden?
- is de beveiliging van de templates voldoende?
- rechtvaardigt het doel een eventuele centrale opslag van biometrische gegevens?

Bijgevoegd is de samenvatting van het rapport.

Reactie BZK op het rapport
In het kader van de ontwikkeling van de Nieuwe Generatie Reisdocumenten wordt de toepassing van biometrie overwogen. Dit voornemen is verwoord in de voorstellen voor de Nieuwe Generatie Reisdocumenten die eind maart van dit jaar zijn aangeboden aan de Tweede Kamer en waar de Kamer op 3 juni jl. in een Algemeen Overleg mee heeft ingestemd.
Het toevoegen van een biometrisch kenmerk aan de reisdocumenten dient twee doelen:

a. als effectief middel tegen 'look alikes' (het gebruik van een reisdocument door een ander dan de rechtmatige houder); dit is een vorm van misbruik die zich steeds vaker manifesteert en naar verwachting verder zal toenemen naarmate reisdocumenten beter beveiligd zijn tegen fraude;
b. het waarborgen van de persoonsgebondenheid bij het gebruik van een elektronische identiteitskaart; een biometrisch kenmerk is daarvoor immers een geschikter middel dan een pincode.

[redacted]

Hiervoor zijn nadere studies en beproevingen noodzakelijk. Momenteel voert TNO een studie uit naar best practises met biometrie en is een aantal pilots voor de beproeving van zowel de elektronische identiteitskaart als - al dan niet gecombineerd- biometrie in voorbereiding. Het verst gevorderd is de pilot die met partners van de sector Sociale Zekerheid (ARBVO, LISV, min. SZW) begin januari 2000 van start gaat. In deze pilot wordt de elektronische identiteitskaart beproefd, die voorzien zal zijn van een biometrisch kenmerk (vingerafdruk) en een elektronische handtekening.

[redacted]

[redacted]

. Vooralsnog zal er in het kader van NGR sprake zijn van een decentrale reisdocumentenadministratie. Dit sluit dus volledig aan bij het standpunt van de Registratiekamer.

[redacted]

- Voor wat betreft de beveiliging van de gegevens, een punt waar ook de Registratiekamer op hamert, moge duidelijk zijn dat dit goed moet worden geregeld. Dit past in het hoge beveiligingsniveau dat zowel voor het fysieke document als voor de elektronische gegevens in het document voor NGR geldt.

[redacted]

[redacted]

N.B. Een enkele keer wordt de elektronische handtekening verward met de gedigitaliseerde handtekening. De gedigitaliseerde handtekening is een fysieke handtekening die gedigitaliseerd is. Zo wordt in het kader van de aanvraag van het nieuwe paspoort in 2001 alle aanvraaggegevens, inclusief de foto en de handtekening, gedigitaliseerd t.b.v. de verzending. Bij het personaliseren worden deze gegevens weer visueel weergegeven.
De elektronische handtekening bestaat uit een cijferreeks.

Spreektekst
Zie bijgevoegde tekst.

Tot slot
De Registratiekamer bestaat 10 jaar. Dit wordt 's avonds ook gevierd. De aanbieding van het biometrierapport staat hier evenwel los van ('slechts toeval').

Bijgevoegd treft u ter informatie een artikel over de elektronische identiteitskaart in de Automatiseringsgids van 1 oktober.

Advies
Kennisnemen van het programma en van de inhoud van het rapport.
Instemmen met onze reactie op het rapport en bijgevoegde spreektekst.

Registratiekamer

Persbericht

's-Gravenhage, 1 oktober 1999

Registratiekamer presenteert biometrierapport

De Registratiekamer presenteert dinsdag 5 oktober om 11.30 uur in Nieuwspoort haar verkenningsrapport "At face value" over biometrische identificatie en privacy aan minister R.H.L.M.van Boxtel van Grote steden- en Integratiebeleid . Na deze presentatie zal een discussie plaatsvinden over het gebruik van biometrische identificatie in het nieuwe paspoort.

PIN-codes en wachtwoorden hebben volgens dit rapport, dat gemaakt werd in samenwerking met TNO/FEL, hun langste tijd wel gehad. Daarvoor in de plaats zal steeds meer gebruik gemaakt worden van biometrische identificatie. Hierbij wordt met behulp van een analyse van lichamelijke kenmerken zoals, stem, vingerafdruk, netvlies of iris vastgesteld dat iemand is wie hij of zij claimt te zijn. Identificatie aan de hand van lichamelijke kenmerken is beter dan een PIN-code of wachtwoord omdat deze kenmerken uniek zijn en niet aan iemand anders gegeven kunnen worden. De Registratiekamer ziet dit als een positieve ontwikkeling omdat systemen daardoor beter beveiligd kunnen worden.

In het rapport "At face value" plaatst de Registratiekamer echter ook kanttekeningen bij deze ontwikkeling. De Registratiekamer wijst onder andere op de gevaren van het centraal opslaan van gegevens. Dit is in veel gevallen niet nodig en de kans op onbevoegd gebruik is erg groot. Daarnaast vindt de Registratiekamer het belangrijk dat identificatiesystemen technisch zo worden ingericht dat een minimale hoeveelheid persoonsgegevens wordt ingewonnen en dat verspreiding van gegevens wordt voorkomen. Ook bij de toepassing van biometrische identificatie in het nieuwe paspoort moet hiermee rekening gehouden worden.

Noot voor de redactie:
Voor meer informatie kunt u contact opnemen met Erik Bogaards tel. 070-3811300

Prins Clauslaan 20
Postbus 93374
2509 AJ 's-Gravenhage
Tel. 070-3811300
Fax 070-3811301

dr. R. Hes
mr. drs. T.F.M. Hooghiemstra
drs. J.J. Borking

With contributions from: P.J.A. Verhaar, T.G.A. van Rhee and
H.A.M. Luijf (TNO Physics and Electronics Laboratory – The Hague)

At face value

On biometrical identification and privacy

Registratiekamer, september 1999

Preface

New ways of doing business are developing at a quick pace. Activities that were once part of our everyday lives are more and more replaced by information technology. In the near future many transactions will no longer be performed by traditional methods, like face-to-face contacts or regular mail. Instead computer networks will be the new vehicles. As persons are physically separated, new and secure methods of identification and authentication are required. The most promising method certainly is biometrical identification, the use of unique human characteristics for these purposes. The widespread introduction of techniques applying biometrics can now be witnessed.

The promise of biometrical identification as a method for secure identification is accompanied by concerns about privacy. The biometrical data, by their nature as unique identifiers, may become a key to track a person's everyday activities. Also the biometrical data may reveal much additional information about a person, such as health status or race.

This report reviews the technologies available for biometrical identification. It also offers guidelines, both from a legal and from a technological perspective, how biometrical identification can be applied in such a way that the privacy of citizens is respected and protected. Applications can be configured to give data subjects the ability to control access to their own biometrical data, to safeguard the integrity of their personal information, and to protect their identity against theft or misappropriation. I hope these guidelines will help to preserve the human face of the information society.

Peter J. Hustinx
Chairman Registratiekamer

Contents

1

Introduction

considerable restraint or even opposition by the potential user community.

One aspect of user acceptance is the concern for privacy. The introduction on a large scale of identification systems that all use the same human characteristic may oblige citizens to present their human characteristic in many circumstances. Such ubiquitous use of the same unique identifier, e.g. a person's fingerprint, facilitates the assembly and accumulation of information related to this person. The human characteristic, potentially, becomes the key with which a dossier tracking a person's private life can be made. Practice shows that such accumulations of personal data will ultimately be used for unintended or even unlawful purposes. Moreover, some human characteristics may themselves contain additional sensitive information, e.g. on race or health and therefore their proliferation is undesirable. Both aspects of these unique identifiers raise considerable concern: the function as a 'universal' key to personal data, and the function as privacy sensitive data. Some analysts sketch the doom of a society where biometrical techniques are applied for omnipresent surveillance.

1.1 A brief outline of the report

The report starts in chapter 2 with a short inventory of biometrics in general and identification or authentication methods using biometrics in particular.

Chapter 3 describes the most relevant legal aspects concerning the application of biometrics. The current legislation on the protection of personal data offers a normative framework to regulate the use of biometrical data. As starting point the issue whether human characteristics come within the scope of the European Directive 95/46/EC is addressed. This study focuses on the practice of identification or authentication with the use of biometrics. A sketch is given how legislation translates into practice for identification with the use of biometrics, adhering to the relevant European legislation. In broad terms the results are valid in all member states.

After the normative framework has been sketched, the report addresses the possibility to limit the amount and use of generated personal data by means of technical solutions, see chapters 4 and 5. The application of Privacy Enhancing Technologies in the domain of identification with the use of biometrics is investigated.

1.2 Studies concerning privacy and technology

The Registratiekamer, in association with TNO-FEL, conducted an earlier study of technologies that could improve the privacy of individuals. The results of that study are published in *Privacy enhancing technologies: the path to anonimity*[1]. A summary of the results of this study is included in Appendix A.

[1] Hes, R. and Borking, J. (editors) e.a. (1998) *Privacy-enhancing technologies: the path to anonimity*. Revised edition. A&V-11. Den Haag: Registratiekamer, 1999.

2

Biometrics: a technology scan

2.1 Biometrics for identification or authentication

It is of importance for the continuity of business processes of organisations to control the access to information systems and buildings. The protection of dat consists of several aspects: the confidentiality, integrity, and availability of the stored data and the integrity of imported data. To ensure the confidentiality, (part of) the integrity, and (part of) the availability of data kept within an information system, only authorised persons should be allowed to gain acces To validate access to the information system, or building the authorisation needs to be inspected. This inspection is practically always combined with the release of the consumer's identity (identification).

To ensure the integrity of imported data the source of these data, and the communication means need to be reliable. To decide whether a source is reliable or not one needs to obtain credentials of the source. As in gaining access to a building or information system, the identity of the source is also released to decide if a source is reliable (identification). The next paragraphs describe how the identity can be verified (identification and authentication) b means of biometrics, and with what human characteristics this can be accomplished.

2.1.1 Identification and authentication

The authorisation, or the reliability of a person is often related to the 'identity of this person. In general this 'identity' is a representation of the person's real identity. In other words: the 'identity' is in fact an entry under which a perso is known to an organisation or an information system. This 'identity' needs tc be unique, to make sure that this 'identity' can univocally be appointed to a particular living person. In order to gain access, or to prove his or her reliability (credentials), a person needs to present his or her 'identity'. This is called 'identification'. With identification, the existence of a specific 'identity' in a reference-source is verified (in case of access control such a reference-source is often called access-control-list).

The 'identity' can be represented by:

1 something a person possesses, like a key or a token (e.g. a chipcard);
2 something a person knows, like a user-id or PIN-code;
3 something a person is, like human characteristics.

Using only identification to grant access, or to declare a person as reliable can cause unnecessary risks. In such cases, 'identities' should be unique and only to be reproduced (for something a person knows), or shown/used (for something a person possesses or is) by the person the 'identity' belongs to. If other persons can reproduce the 'identity', these persons can gain access und a false 'identity'. The loss of a token (something a person possesses), or the

combined with a human characteristic (something a person is) for authentication;

4 a token (something a person possesses) for identification combined with a human characteristic (something a person is) for authentication;

5 a token (something a person possesses) for identification combined with a PIN-code or a password (something a person knows), and a human characteristic (something a person is) for authentication.

Identification (and authentication) can be implemented in several ways, although these ways are subject to two limitations. The implementation extremes are incidental identification (and authentication) and continuous identification (and authentication). With incidental identification, the 'identity' of a person is only checked when gaining access to a building or information system. The same goes for deciding whether a source is reliable. Only at the beginning of a session the 'identity' is checked. When a person has accessed a building or information system, however, someone else can take over the activities of the identified person. This can be prevented using periodic or continuous identification (and authentication). With periodic identification, the 'identity' will be checked frequently during the presence in the building or information system, or during the existence of the session. When using continuous identification, the 'identity' is checked every moment (continuously) during the presence in the building or information system, or during the existence of the session. Some human characteristics in particular like the voice, or keystroke patterns, can be used to carry out continuous identification (and authentication).

2.1.2 Working of products

The system for using biometrics for identification or authentication consists of:

1 a sensor that records the human characteristic that is presented;

2 a verification device that identifies a user (identification), or verifies the identity of a user (authentication);

3 a template database where reference material for the identification or authentication of users is stored.

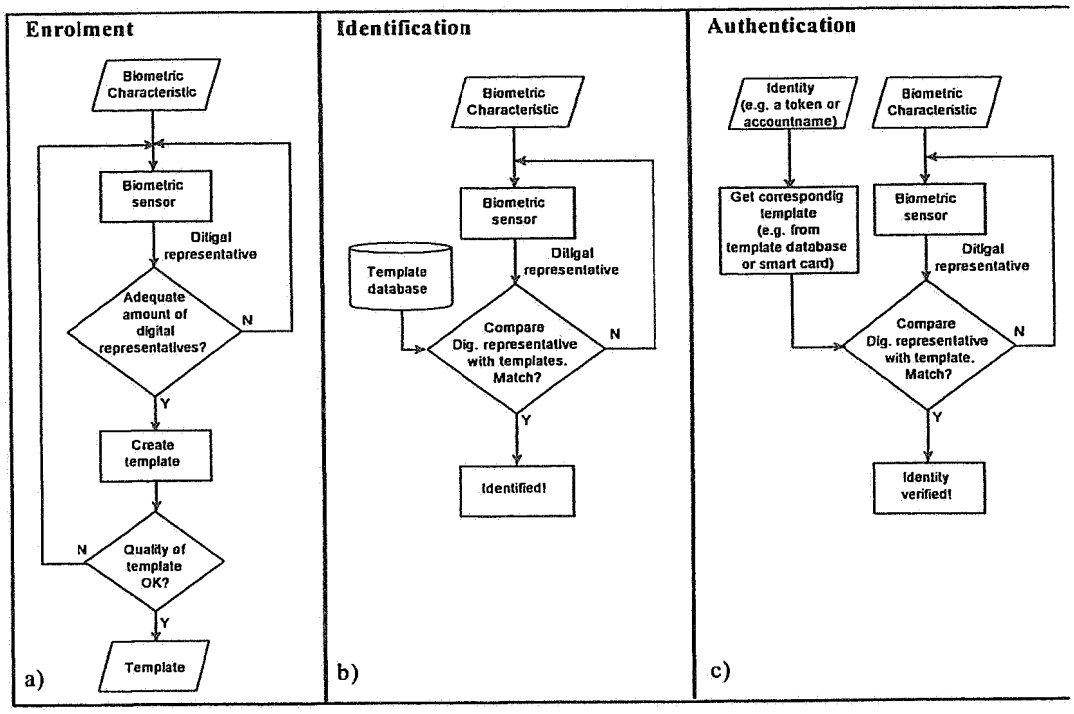

Figure 2: Possible diagrams for the enrolment phase and the operational phase: a) enrolment phase; b) operational phase of a system that uses biometrics for identification; c) operational phase of a syster that uses biometrics for the verification of a given identity (authentication).

As mentioned before, two phases can be distinguished: the initialisation pha or enrolment phase, and the operational phase. During the enrolment phase, the system will define the templates of the users, while during the operation phase the system will identify or authenticate the users. Possible diagrams o these phases are given in figure 2.

During the enrolment phase, which is illustrated in figure 2.a, the template t is used as comparative material for the identification or authentication is created. First the human characteristic of a person has to be presented to the sensor. The sensor converts the human characteristic into a digital representation and records this. When creating a template, the conversion of the human characteristic into a digital representation has to be executed mor than once. The similarities from the several digital representations are used t create the template. Figure 3.a gives a simplified example of how digital representations are used to create a template. The corresponding digits (bits) from the several digital representations that are equal to each other are used the template. Corresponding digits that are not equal will not be used, and a illustrated in figure 3.a as an 'x' in the template. The 'x' can be seen as 'don't care' digits. The value of these digits is of no importance to the identification authentication of individuals. After the template is created, the quality of the template needs to be checked. The template needs to contain enough digits t

temperature variations and the presence of dust; and behavioural conditions such as stress and sweat.

A rejection by the system of someone truly linked to the template used for comparison is called a 'false rejection', and will decrease user acceptance of such a system. An acceptance of someone who doesn't belong to the template used for comparison is called a 'false acceptance', and could cause a security violation. The technical specifications of these tolerances are given with the 'False Rejection Rate' (FRR) and the 'False Acceptation Rate' (FAR). These two rates are related as illustrated in figure 4.

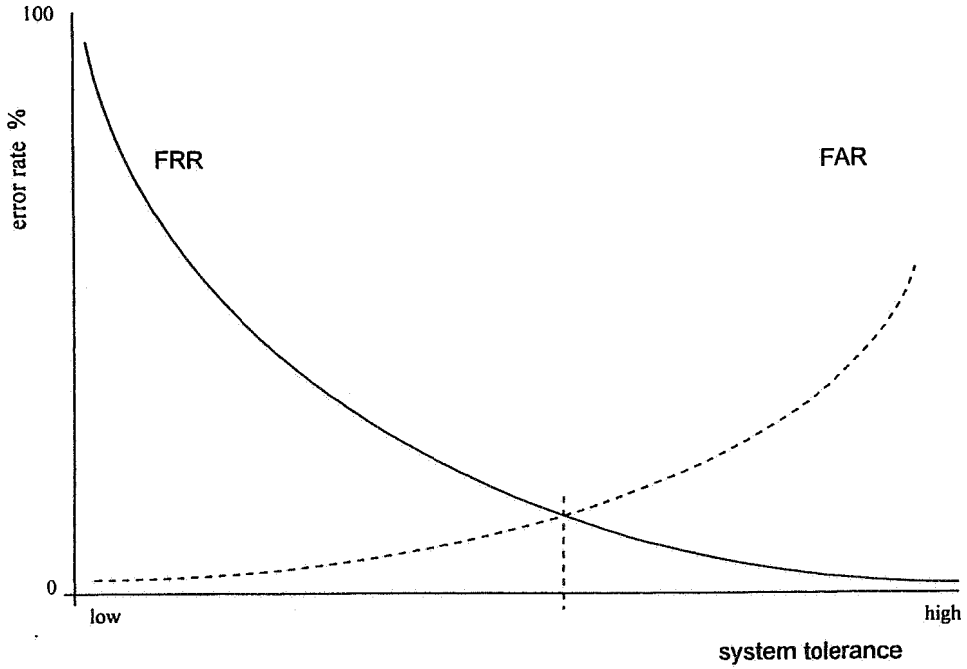

Figure 4: Relationship between FAR and FRR. The vertical axis represents the fault tolerance for the FAR and the FRR expressed in percentages. The horizontal axis represents the system tolerance that can be adjusted.

The default settings of most products are adjusted so that FAR = FRR. As shown in figure 4 it is clear that if the FRR is low, the FAR will be high, and if the FRR is high, the FAR will be low. With a product that is adjusted in such way that authorised users will rarely be rejected (FRR is low), the chance that unauthorised persons gain access will increase (FAR is high). A product that denies access to all unauthorised persons (FAR is low) needs to be very accurate. Such an accurate product will lead to an increased chance of the rejection (FRR is high) of authorised users. Depending on the security requirements of the system, in which the product that uses biometrics is integrated, these settings can be adjusted to obtain the required security level.

customer used the right fingerprint, so the banking services have to perform as if nothing is the matter. Meanwhile, actions to protect the banking services and the safety of the customer will be (need to be) taken.

Hand scans

The following details of the hand can be used for identification: finger length, the lines of the palm print (equal to a finger print), vein patterns on the back of the hand, hand geometry and finger geometry. For the method of vein recognition, a two-dimensional scan is made of the vein pattern. This scan will be transformed into a grey-scaled picture, and then stored in a template.

In case finger and hand geometry is used, the 3-dimensional shapes of respectively the finger and hand is captured. Details that can be used with hand geometry are the length of the fingers, the thickness of the hand, the shape of the hand and the brightness of the skin. The same details are measured for finger geometry, but only for two fingers instead of an entire hand. By measuring the brightness of the skin some information about the colour of the skin and probably the race can be extracted during the process of scanning. Contrary to the fingerprint, finger and hand geometry is not susceptible to incisions and chaps. Finger and hand geometry can still be influenced by major injuries of the fingers and the hand, and environmental conditions, such as dirt.

For finger and hand geometry, products are available (e.g. Digi-2 by BioMet Partners, and ID3D Handkey by Recognition Systems Inc.). Products that use palm print for identification or authentication are also available. DermoTrade offers the product Automatic Dermatoglyphical Identification System, which uses the palm print for identification. The Papillon-7 (Papillon Systems), and RECOderm system (KFKI Computer Systems) are also products that use the palm print for identification, or authentication. For vein pattern recognition there are advanced developments that may lead to the release of products in the near future.

Eye patterns

One of the best ways of identification can be obtained by using certain characteristics of the eye. Both retina and iris contain unique and stable details that can be used for identification. With respect to privacy it could theoretically be possible to deduce sensitive information about the health of users because certain diseases influence some features of the eye. Iridology e.g. is a form of diagnostics, which makes it possible to recognise diseases by tracing abnormal spots, lines, and features in the iris. Official medical science attaches little value to iridology. This, however, may not reflect the opinion of many individuals, who may resist biometrical identification on basis of their belief in iridology or similar types of diagnostics.

Body scent

This characteristic consists of approximately thirty chemical substances that form a specific unique scent for every individual. An electric nose can be built, consisting of a number of chemical receptors that generate a difference in voltage in case a particular chemical substance is present. With the help of neural networks it is possible to disentangle specific scent patterns.

At this moment there are no commercially available products. Mastiff Electronics is developing a product that will probably be launched around the beginning of the new millennium. The Tufts University is discussing the commercialisation of a scent recognition system developed by laboratories in the chemistry and neuroscience departments of this University.

DNA

All human cells, except for the red corpuscles, contain a core of genetic information, which is unique for every individual. This is called DNA. Identification or verification using DNA is often used in forensic laboratories. The amount of material needed for such an analysis is very small; e.g. one hair is sufficient. At this moment, there is still a strong resistance against the use of DNA for identification and/or authentication in more common applications. This resistance lies in the fact that human cells need to be taken from the human body, as well as the potential (mis)use of additional information contained in the DNA.

Signature

Seals and signatures are behavioural characteristics and have been commonly used to identify the originator and to verify the authenticity of documents. There exist two methods to identify a person based on signatures. The first method compares already written signatures with a signature from a reference-source. The second method examines the dynamics of the signature when it is written down. Details of this characteristic are the writing rhythm, contacts on the surface, total time, turning point, loops, slopes, velocity and acceleration, and pen pressure. It is very difficult to imitate a signature that is controlled dynamically.

Most of the commercially available signature systems, and signature systems under development are based on dynamic signature verification. There are about ten products commercially available, and about the same number are under development.

Voice

As mentioned before, people can recognise acquaintances by listening to their voices. A voice obtains its unique character because of the unique sizes of the nasal cavity (or nasal passage), pharynx and mouth. Machines can recognise unique details of the human voice that cannot be heard by humans. It is

and is integrated in the NetNanny software suite. There are a couple of universities and research laboratories that study keystroke dynamics, and are developing identification, or authentication systems using this technology. TNO-FEL in the Netherlands is one of the laboratories that develop a system based on keystroke dynamics.

2.1.4 Comparison of reliability of different techniques

Figure 5 shows a comparison of biometrics techniques with respect to several (most used) characteristics. Although the table does not capture all relative advantages and disadvantages, it does show that each characteristic has relative merits.

	Reliability	*Acceptance*	*Template*	*Costs*
Fingerprint	good	good	small	low
Hand	good	good	very small	moderate
Eye	very good	moderate	moderate	high
Face	good	good	small	moderate/high
Signature	moderate	very good	small	moderate
Voice	good	good	small	low
Keystroke	moderate	good	small	low
DNA	very good	poor	moderate	high

Figure 5: Comparison of biometrics techniques with respect to several characteristics.

As for reliability, all techniques will perform well under ideal conditions. However, reliability rates suffer under less than ideal conditions. The eye has very good reliability rates, where signature and keystroke have moderate rates. With respect to the acceptation of biometrics techniques the signature scores well, because it is used in a way similar to traditional signing. The acceptation of the eye scan methods is moderate because of the required short distance between the user's eye and the sensor. The next column, on the size of the reference template, shows that hand-scanning can work with small templates. Because the eye requires highly detailed pictures the particular template is fairly large. The last column represents a general overview of the costs of the biometrics systems. Most techniques are now available at reasonable costs, except eyescanning and determination of the facial heat pattern, which are relatively expensive.

2.1.5 Acceptance of biometrics for identification and authentication

The success of using biometrics for identification or authentication depends not only on technical specifications such as performance, reliability and stability, but depends also on the acceptance by the (future) consumers. One

'state of mind', the former are mostly used in the scientific literature. This is because emotion has a solid correlation with the techniques used for detection of deception, with e.g. a voice stress analyser.

According to Webster's ninth new collegiate dictionary the following definitions can be applied to the terms 'emotion' and 'mood'. "Emotion: A psychic and physical reaction (as anger or fear) subjectively experienced as strong feeling and physiologically involving changes that prepare the body for immediate vigorous action." "Mood: A conscious state of mind or predominant emotion", or "A receptive state of mind predisposing to action."

In *Toward the simulation of emotion in synthetic speech*[5], the following distinction is made regarding to 'emotion' and 'mood': "Emotions arise suddenly in response to particular stimuli, and last for seconds or minutes, while moods are more vague in nature, lasting for hours or days. Although the onset of an emotion can usually be readily discerned from a preceding mood, it is impossible to define when an emotion becomes a mood; possibly for this reason, emotion is very often used as a general term incorporating the concept of mood also." Therefore, we will use the term 'emotion' for the purpose of state of mind in this report.

Emotions can be expressed in several ways, and with several human characteristics, or combinations of these characteristics. Human characteristics that have strong relations with emotions are e.g. the human face, the human skin, body scent, the placing of signatures, and the voice. It is possible to read from the look of someone's face in what emotional state that person is. It is also possible to recognise emotions when a person speaks. The human skin reacts on emotions by creating more sweat. This principle is used to create lie detectors. As stated earlier, the static and dynamic signature and the analysis of keystrokes are behavioural characteristics and are susceptible to the emotional state of a person.

Because voice recognition will be described in more detail to examine the privacy risk of biometrics, this study will focus on the determination of emotional expressions in the human voice.

[5] Murray, I. and Arnott, J. (1993) *Toward the simulation of emotion in synthetic speech: A review of the literature on human vocal emotion*. Acoustical Society of America. (2) February 1993, p. 1097-1108.
6 Keifer R. (1966). *Polygraph versus voice stress*. September 11. www.polygraph.org.

How are emotions expressed in the human voice

Before the emotional expressions in the human voice can be described, clarity should exist on the various emotions and the way they originate. In Keifer, Polygraph versus voice stress,[6] the following four basic emotions are addressed: happiness, sadness, anger and fear. All occurring emotions can be seen as a combination of one of these four basic emotions plus the information about what caused it, or to whom it is directed. Several scientists have come up with the following three-dimensional model:

associated with the stress of deception. These changes include alterations in the heart rate, breathing, and electrodermal activity (emotional sweating). Other changes occur as well: the pupils get larger, digestion slows, the body's blood supply is redistributed away from the skin and gastrointestinal regions and toward the muscles, etc.[8]. These measurements are performed by several consecutive physical tests by connecting the subject to multiple sensors simultaneously[9]. The measures used by the polygraph were selected in the 1920s and 1930s because they were simple to record (as opposed to brain waves and gastrointestinal activity), they were sensitive, and they were accurate[10].

About 25 years ago, serious efforts were made to analyse the human voice for the detection of deception. Meanwhile many devices are widely being marketed. Voice analysis offers many advantages over current polygraph methodology. Examinations can be conducted remotely, using a telephone, and shifted in time, using a tape recording. Voice samples can be recorded without discomfort to the subject, and can also be conducted surreptitiously and would be of great benefit in intelligence and counterintelligence investigations. But of course, the most important is the accuracy of such a device. To date the methods of voice analysis are not accurate enough to replace the existing polygraphs[8].

Focused on the use of the human voice, Keifer[9] describes a correlation between the so called primary emotions (anger, happiness, sadness, fear and disgust) and some vocal effects (speech rate, pitch average, pitch range, intensity, voice quality, pitch changes, articulation). In the following figure these correlations are summarised.

[8] *Truster, your personal truth verifier.* User guide.
[9] Keifer, R. (1996) *Polygraph versus Voice Stress.* September 11, (www.polygraph.org.)
[10] Murray, I. and Arnott, J. (1993) *Toward the simulation of emotion in synthetic speech: A review of the literature on human vocal emotion.* Acoustical Society of America. (2) February 1993, p. 1097-1108.

	Anger	*Happiness*	*Sadness*	*Fear*	*Disgust*
Speech rate	slightly faster	faster or slower	slightly slower	much faster	very much slower
Pitch average	very much higher	much higher	slightly lower	very much higher	very much lower
Pitch Range	much wider	much wider	slightly narrower	much wider	slightly wider
Intensity	higher	higher	lower	normal	lower
Voice quality	Breathy, chest tone	breathy, blaring	Resonant	irregular voicing	grumbled, chest tone
Pitch changes	abrupt, on stressed syllables	smooth, upward inflections	downward inflections	normal	wide, downward terminal inflections
Articulation	tense	normal	slurring	precise	normal

Figure 7: "Summary of human vocal emotion effects. The effects described are those most commonly associated with the emotions indicated, and are relative to neutral speech" [8]

seconds.[13] This change in performance can be explained by the increase in computer power, such as processor speed and access times for disk and memory and improved compression algorithms.

If this trend persists, the following decade will result in an average estimated time for a template match of 2 seconds, and an average template size of approximately 30 bytes.

With respect to biometrics used for identification or authentication, it is expected that, especially for demanding applications, different human characteristics can be combined into multi-technique systems. It can be assumed that a person's fingerprint is independent from his/her eye pattern, so multi-technique systems can provide a better reliability. At this moment the Dutch Government studies the integration of the identification card with biometrics.[14]

With respect to biometrics used to expose emotions, it is expected that characteristics like voice, face and keystroke dynamics will have great influence, because these characteristics can be measured without the notice and consent of the persons involved. Especially, when working in multimedia spaces, where during a video-conferencing session all movements, can be seen by each of the participants, human characteristics including body language, can give more information than is intended.[15] The measurement of exposed emotions may be of value for electronic commerce, to influence the purchase pattern of customers. This will be stimulated by the earlier mentioned integration of biometrics with multi-media systems.

[13] Rhee, T. van and Verhaar, P. (1997) *Tokens en biometrie voor identificatie en authentificatie*. TNO-FEL-97-A003, Den Haag.
[14] Ministerie van Justitie. (1998) *Nota wetgeving voor de elektronische snelweg*. Tweede kamer, Kamerstuk 25880, 1997-1998.
[15] Agre, P. and Rothenberg, M. (eds.). (1997) *Technology and Privacy: The new landscape*, MIT Press.

3

Legal aspects

measurements of certain features in a fingerprint and the storage of these in a table. A next stage could be the mathematical transformation of these data into a code.

There is no reason to think that what applies to the human characteristic itself, would not apply to the digital representation of that characteristic, the templates which are composed on the basis of these representations, and to any subsequent transformation. As the process continues, the amount of detail will change, but the unique link with the person concerned is kept. It is reasonable therefore to conclude that the data involved will remain personal data in most, if not all stages of their processing.

To determine whether or not the Directive is applicable, the question has to be answered when personal data is processed, and whether the way in which personal data is used falls within the scope of the Directive.

3.2 Processing personal data

The definition of the term 'processing' in article 2(b) the Directive is fairly broad:

Article 2 (b) of the Directive:
'Processing of personal data' ('processing') shall mean any operation or set operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

For example, identification using biometrics may involve the processing of personal data when an algorithmically processed biometrical data item (like e.g. a template) is stored or if information on a network is forwarded, as illustrated in figure 8 in chapter 4, of a 'hand geometry verification system that replaces the PIN code verification of a (credit) card banking system'.

3.3 Scope of the Directive

Article 3 (2) of the Directive:
This Directive shall not apply to the processing of personal data by a natural person in the course of a purely personal or household activity.

Thus, the Directive does not apply to purely personal activities, even when personal data is concerned. Arguably, some ways of authentication by means of biometrics can be considered as such.[2]

[2]The approach taken here, where it is considered if there is use of personal data as a personal activity would appear to us to be more effective then the approach used in the Dutch ITeR report '*Het lichaam als sleutel, juridische beschouwingen over biometrie*' (1997) which argues that there is no personal data in this context. (Kralingen, R. van , Prins, C. and Grijpink, J. (1997) *Het lichaam als sleutel.* IteR, Vol. 8, Samson).

(c) Processing is necessary for compliance with a legal obligation to which the controller is subject

or

(d) Processing is necessary in order to protect the vital interests of the data subject,

or

(e) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed,

or

(f) Processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection.

Article 6 (a) for example means that the processing and collection of data must be done fairly. Hence, people have to be aware that identification by means of biometrics is used. Also article 10 is of importance in this respect, see section 3.5. Article 6 (b) means that when biometrical data for identification is processed with the aim of determining whether or not somebody is permitted to access a given system, the use of this data to determine the emotional state of the person concerned, or his or her race would in principle not be compatible with the purpose specified to the subject, i.e. biometrical identification. Furthermore, the objective of processing that personal data should be justified in accordance with article 7. The processing of the data is permitted if at least one of the conditions listed in article 7 is fulfilled.

3.5 Information to be given to the data subject

According to Article 10 of the Directive the controller has to provide the data subject from whom data relating to himself are collected, with at least the following information:

10(a) The identity of the controller and of his representative, if any;

10(b) The purposes of the processing for which the data are intended;

10(c) Any further information such as
- the recipients or categories of recipients of the data,
- whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply,
- the existence of the right of access to and the right to rectify the data concerning him, in sofar as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.

Exemptions may only be granted in clearly defined cases:

8(2)a The data subject has given his explicit consent to the processing of those data, except where the laws of the Member State provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject's giving his consent; or

8(2)b Processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorized by national law providing for adequate safeguards; or

8(2)c Processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent; or

8(2)d Processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or other non-profit-seeking body with a political, philosophical, religious, or trade union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third without the consent of the data subject; or

8(2)e The processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise, or defence of legal claims;

8(3) Paragraph 1 shall not apply where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.

8(4) Subject to the provision of suitable safeguards, Member States may, for reasons of substantial public interest, lay down exemptions in addition to those laid down in paragraph 2 either by national law or by decision of the supervisory authority.

The giving of 'consent' referred to in article 8(2)a should comply with the definition of the Directive (article 2h):
'the data subject's consent shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed'

Taken together, for systems using biometrical identification or authentication, the main boundary conditions are as follows. If raw or processed biometrical data is considered as sensitive data, in principle the processing is prohibited. Ir some cases the processing can still be justified if explicit consent is given. The

4

Biometrical identification and privacy-related issues

relevant. This chapter will address privacy issues related to the use of biometrics for identification, or authentication, and, to a lesser extent, for determining emotional states.

4.1 Biometrics for identification and authentication

In case of biometrics, the human characteristic measured is personal data that is uniquely related to the identity of a person. The linking of databases using the biometrical data as key, is a manifest risk as soon as a person uses a human characteristic to enrol to a system that uses biometrics for identification or authentication.

It should be noted that human characteristics can also be used in such a way that enrolment, identification or authentication take place without the persons involved being aware of it. Thus, the following cases should be distinguished: it is known that enrolment, identification or authentication takes place, or; it is not known that enrolment, identification or authentication takes place[1].

It is possible that persons are being identified or authenticated without being aware of it. There are several characteristics, like voice, keystroke, face, and body scent, that can be used in such a way that persons do not notice they are being identified or authenticated. This potentially leads to an undesirable type of secret surveillance.

As mentioned in the previous chapter, such collection without informing the persons involved is generally not allowed, because personal data must be processed fairly and lawfully (article 6a of the Directive). Moreover, article 10 of the Directive (see section 3.5) states that in case of such a collection of personal data the controller, the person or organisation applying the biometrical identification technique, has to reveal his identity.

4.1.1 Known identification or authentication

In this case, when enrolment, identification, or authentication processes use human characteristics, a person will recognise the moment that he is identified or authenticated, because he needs to present his characteristic in a specific way.

Imagine that the PIN-code used by banks for the authentication of their clients at ATMs is replaced by hand geometry verification. With the conventional (credit)card and PIN-code the clients could adopt, to some extent, pseudo-identities[2], by using different (credit)cards and PIN-codes. Because most products using hand geometry for identification or authentication are based on the right hand, changing pseudo-identities is not possible. Changing pseudo-identities is also pointless when using the same characteristic for identification

[1] Borking, J. and Verhaar, P. *Biometrie und Datenschutz, Bedrohungen und privacy-enhancing technologies* in DUD (Datenschutz und Datensicherheit) no. 3/1999, p. 138-142.

[2] Hes, R. and Borking, J. (editor) a.o. (1998). *Privacy-enhancing technologies: the path to anonimity*. Revised edition. A&V-11, Den Haag: Registratiekamer.

Telephone companies, e.g., are looking for ways to identify or authenticate customers that want to use electronic commerce services offered by the phone-company, by means of their voice. In telecommunications there is a growing need for strong identification and authentication mechanisms[3] in particular because of the geographical separation of parties connected by the telecommunications network. Also there is the need to fight the annually increasing levels of fraud. Phenomena like the cloning of mobile telephones (stealing the ID of a handset and copying it into another), enrolling for services under an alias without paying, and theft of subscriber lines from telephone exchanges can be mentioned. Voice or speaker recognition is a method that can be used for identification and authentication, and can be used to control access to the network and equipment, and access to the services delivered over the network.

At this moment, without the use of biometrics, a person who makes a telephone call using his own static telephone connection, or mobile phone, will automatically identify himself because of the subscriber-number. If the subscriber allows another person to use his telephone connection this other person will be identified as the subscriber. Authentication can take place by using PIN-codes, passwords, or pass-phrases, but these can be exchanged, or filched, so there is no real assurance. A person can make anonymous calls by using a pay-phone (public-phone).

When voice recognition will be introduced, it will be helpful against misuse of telecommunication services, but it will also limit the possibility for individuals to remain anonymous. Again, the human characteristic used is unique, and therefore, the telephone company could make a profile of each customer. It is also possible to use a system to identify customers instead of only verifying their identities. When the voice is used to identify customers, it will be more complicated to make anonymous calls at a later stage (see figure 9).

[3] As for services delivered by means of the telecommunication networks, identification of customers is increasingly seen as an important element of sales and marketing. Having been identified unambiguously, personal data on an individual can be retrieved from databases and used for making on-line decisions on the way a person is treated. Also, a person's mental or emotional state derived from his or her voice can be used for sales and marketing purposes. Real-time analysis can potentially be used in a commercial context to influence behaviour of a client, e.g. in telephone sales. Whether this will become significant from a business perspective is difficult to judge; it has to be noticed that it can create a situation of asymmetry in which the client is not asked for consent.

tolerance results in the 'false rejection' of authorised persons, and in the 'false acceptance' of unauthorised persons. The technical specification of this tolerance is given with the 'False Acceptance Rate' (FAR) and 'False Rejection Rate' (FRR).

These two rates are related, see figure 4. If the FRR is low - few persons will be falsely rejected -, the FAR will be high - some unauthorised persons will be falsely accepted -, which means that the accuracy of the measurement will be low. However the user acceptation will be high. If the FAR is low - few unauthorised persons will be falsely accepted -, the FRR will be high - some persons will be falsely rejected -, which means that the user acceptation will decrease. In this case, the measurements will be accurate. Both false rejection and false acceptance can lead to privacy-related problems.

False rejection and social acceptance

It is known that certain groups of persons have human characteristics that are less pronounced than average or different in such a way that automated biometrical identification is not working properly with the current products. Such groups have an overall higher risk of false rejections. Potentially this can have a discriminatory effect if e.g. denial of service happens more often to members of such a group. The false rejection of someone, e.g. an employee in front of his or her colleagues, can also lead to unwanted reactions. These social aspects are of vital importance when introducing a new technology.

False acceptance and the quality of personal data

The false acceptance of an unauthorised person means that this person is granted access to a building, object, or information system on account of an authorised person. The personal data that will be collected will be assigned to the authorised person, and therefore, the quality of this person's personal data is affected. Maintaining the quality of personal data in an element of data protection and therefore, also from a legal perspective, relevant to the privacy discussion. See article 6(1)d of the Directive concerning the quality of personal data, and article 17 of the Directive concerning the required security measures to protect the quality of the data.

It is important to stress that, when biometrical systems are used, there is always a fraction of false acceptances. Corruption of personal data due to false acceptances will occur. The use of biometrics however might create the illusion that the personalization is always correct.

5

Biometrics and privacy-enhancing technologies

In such cases where no alternative is present, the system should be equipped with some form of PET in order to guarantee the individual a certain level of protection of his personal data. The system owner is responsible for the integrated PET. In this case the measures could be:

1 decentralising of the template storage, and verification;
2 encryption of template-databases (in case of template storage in central databases).

5.1.1 Decentralising template storage and verification

By decentralising both the template storage and verification process, the biometrical data will be processed in an environment controlled by the individual or an environment from which no connection to a central database can be made.

Decentralised storage and decentralised verification on a token
When decentralising the template storage and verification of the presented human characteristic, it is necessary that the template and the verification process can be adequately isolated from the rest of the access control system. Using a chipcard, the template can be stored on the card and the comparison of the template and the card can handle the digital representation. The sensor also (and the rest of the biometrics product) needs to be tamperproof, so malicious bank employees, or shop employees can not retrieve the digital representation, or the template. The customer is anonymous and none of the generated data can be linked to other data concerning his or her identity. Therefore, it would be ideal if the sensor and chipcard could be integrated. Recent developments demonstrate that it is possible to integrate the sensor with the chipcard[1]. Figure 10.a illustrates a possible implementation of such a product, while figure 10.b illustrates a product with a sensor that is integrated with the service.

Figure 10 describes the process of the identification or authentication to gain access to a certain desired service. In figure 10.a the human characteristic is recorded by the chipcard. The chipcard compares the obtained digital representation with the template, which is already stored on the chipcard. In this way all biometrical data (both the digital representation and the template) stay on the chipcard. The only information exchanged between the chipcard and the service is a positive or negative result of the identification or authentication process executed by the chipcard. This is illustrated by the authorisation code.

This case can legally be interpreted as a case of personal use, see paragraph 3.3 of chapter 3, following article 3(2) of the Directive. If this situation can be created, the person can stay anonymous to the system, and the processing of these data is outside the scope of the Directive.

[1] HSB cards and Cards Systems, Woerden, The Netherlands, private communication.

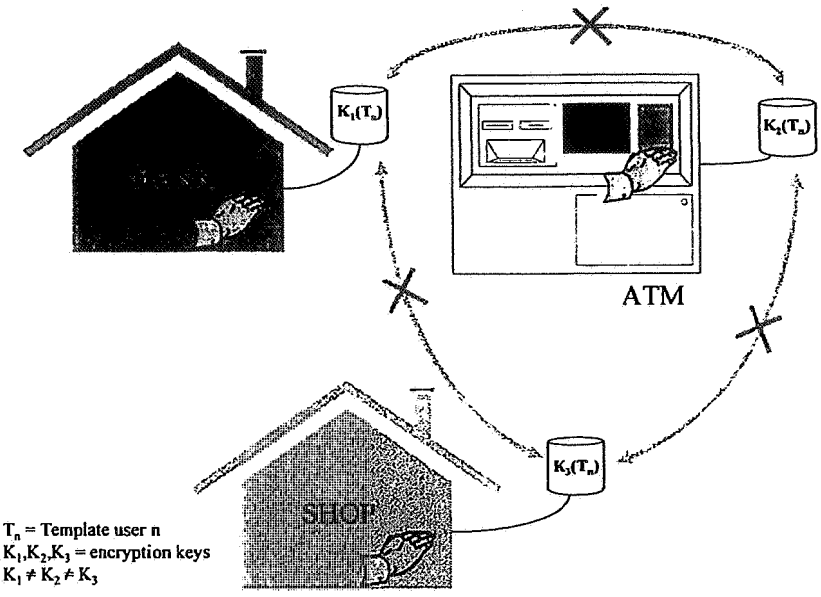

Figure 11: The use of mathematical manipulations such as hash-functions or encryption algorithms can prevent incompatible use of biometrical data. This method will protect the privacy of customers by protecting the recorded personal data against incompatible use.

Theoretically, the best way to do so is the use of one-way-hash-functions.[2] Before the template is stored in the template-database, the template is processed with this hash-function, generating a hash-value of the template. This hash-value will be stored in the template database. When verification of a human characteristic is needed, the digital representation of the characteristic will be hashed, resulting in a hash-value of the characteristic. If the hash-value of the template matches the hash-value of the characteristic the person involved is identified or authenticated. This method, unfortunately, will not work properly in practice, because of the difference that might occur between the digital representation of the human characteristic and the stored template, see also chapter 2.

Encryption is also an important instrument for protection of data. Every product needs to use different encryption and decryption keys to prevent the combination of personal data from different (template-)databases, see figure 11. A problem arises when encrypted templates are compared to encrypted representations, because of the possible differences between templates and representations. Therefore, the encrypted templates stored in the template-database need to be decrypted before they will be compared to the plain digital representation of the human characteristic. To prevent others from taping the digital representation, or the plain template, and replaying these, the products need to be tamperproof.

These measures can be used for each biometrics system using any human characteristic.

[2] A hash function is a mechanism for mapping messages of arbitrary length to messages of small fixed length. These so-called hash-values of the message are intended to serve as compact representation images of the messages themselves. A basic requirement on hash functions is that they must be difficult to forge, i.e., knowledge of a hash-value alone should not allow the effective computation of a pre-image, i.e., a message that maps to this hash-value. One distinguishes between keyed hash functions (the so-called Message Authentication Codes (MACs)), i.e., hash functions that can be reconstructed once a secret value is known, and unkeyed hash functions (the so-called Modification Detection Codes (MDCs)), i.e., publicly known hash functions. Hash functions are usually denoted by the symbol h (or h_k, if it is a keyed hash function). If one uses this algorithm, the hash value provided over a message m is denoted by $h(m)$ (resp. $h_k(m)$).

5.2 Unknown identification or authentication

We noticed in chapter 3 that the Directive obliges organisations to announce whether personal data, including biometrics, are collected when a person uses a certain system; e.g. when making a telephone connection to a service using voice recognition, an announcement should be made, before the actual identification or authentication takes place.

When it is not known to a person whether he is being identified or authenticated, he can take preventative measures himself. A possibility is the use of scramblers that modify the human characteristic in such a way, that he cannot be identified or authenticated. A person can use voice scramblers, in a preventative way, when he is not sure about whether or not the system will execute an identification or authentication. This 'digital handkerchief' should scramble the voice of the person in such a way that each time the scrambler is used a different voice is heard. This method can only be applied to products that use the human voice for identification or authentication. There are no practically feasible measures to protect individuals from identification or authentication by products using other human characteristics.

Resuming, the instruments an individual has to influence whether his characteristics are collected are quite inadequate. The responsibility of designers of biometrical systems, and of the organisations wishing to apply these, should therefore be stressed.

6

Conclusions and practical directions

data, it may be necessary to create a specific legal basis with all appropriate safeguards.

Besides these issues related to personal data, other privacy issues are relevant when biometrical identification or authentication is applied. These are:

5 Each human characteristic is unique, and therefore its digital representation or template can be used as a key to search databases that contain other personal data;
6 Certain human characteristics can be used for identification, and for other purposes such as the exposure of emotions, without the knowledge and the consent of the persons involved;
7 The quality of personal data can be at risk, because of the technical restrictions of the technology.

6.1 Recommendations

To minimise or eliminate the impact of privacy risks associated with biometrics, the following measures should be taken:

1 Analysis of the need for biometrical identification or authentication. Is the application of biometrics proportional with the goal to be achieved?
2 Decentralisation of the template storage and verification process;
As a rule both the storage of templates and the verification process should be decentralised. In some specific cases and environments, the processing of personal data can be seen as a pure personal activity.
3 Encryption of databases: the protection of personal data can be realised by using different encryption keys and algorithms to encrypt the personal data (including biometrical data) in different databases. The original biometrics should preferably be destroyed after the derivation of the digital template;

The individual whose human characteristics are measured may consider the following:

4 Use of different characteristics: the previous countermeasures should be integrated into the system. If a system does not contain any countermeasures, individuals can use different pseudo identities and different human characteristics to identify and/or authenticate themselves;
5 Use of scramblers: just like the use of different characteristics, individuals could use scramblers to randomly distort the results of the recording of the characteristic. This countermeasure can only be used for certain characteristics, like the voice.

Certification of the privacy-compliance of products will guarantee an adequate handling of the personal data of future users.

Designers, developers, suppliers, and users of products using biometrics for identification, authentication, or exposure of emotions need to consider ways

Appendix A Privacy-Enhancing Technologies

Conventional information systems generally record a large amount of information. This information is often easily linked to an individual. Sometimes these information systems contain information that is privacy-sensitive to some individuals. To prevent information systems from recording too much information the information systems need to be adjusted.

There are a number of options to prevent the recording of data that can be easily linked to individuals. The first is not to generate or record data at all. The second option is not to record data that is unique to an individual (identifying data). The absence of such data makes it almost impossible to link existing data to a private individual. These two options can be combined into a third one. With this third option, only strictly necessary identifying data will be recorded, together with the non-identifying data.

The conventional information system contains the following processes: authorisation, identification and authentication, access control, auditing and accounting. In the conventional information system, the user's identity is often needed to perform these processes. The identity is used within the authorisation process, for instance, to identify and record the user's privileges and duties. The user's identity is thus introduced into the information system. Because in a conventional information system all processes are related, the identity travels through the information system.

The main question is: is identity necessary for each of the processes of the conventional information system? For authentication, in most cases, it is not necessary to know the user's identity in order to grant privileges. However, there are some situations in which the user must reveal his identity to allow verification of certain required characteristics.

For identification and authentication, access control and auditing the identity is not necessary. For accounting, the identity could be needed in some cases. It is possible that a user needs to be called to account for the use of certain services, e.g. when the user misuses or improperly uses the information system.

The introduction of an Identity Protector (IP), as a part of the conventional information system, will structure the information system in order to protect the privacy of the user[1]. The IP can be seen as a part of the system that controls the exchange of the user's identity within the information system. The IP offers the following functions:

1 Reports and controls instances when identity is revealed;
2 Generates pseudo-identities;
3 Translates pseudo-identities into identities and vice versa;
4 Converts pseudo-identities into other pseudo-identities;

[1]See also Common Criteria for Information Technology Security Evaluation. Version 2.0. Part 2, chapter 9, Class FPR: Privacy. ISO IS 15408 (8 june 1999).

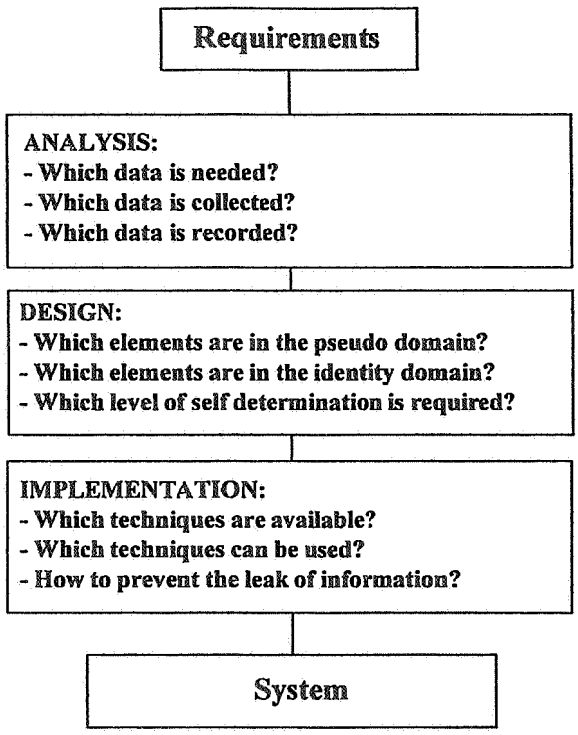

Figure 15: Aspects to take into account during the different phases of the design process of a privacy information system

Human characteristics, such as fingerprints and eyes, are increasingly being used for identification and authentication of persons. Such techniques for identification and authentication techniques are now being introduced for common purposes, like access control to buildings, personal computers, or commercial services.

The uniqueness of each human characteristic will help to ease many problems inherent in traditional methods of identification and authentication. This is especially relevant because, nowadays, more and more transactions are being performed without direct contact between the parties involved, making use of computers and computer networks. Increased security of transactions, ease of use and a better control of fraud are strong arguments to use human characteristics for identification. This form of identification or authentication is also known as biometry, or biometrics.

The widespread use of biometrics is, however, accompanied with a major concern for the privacy of the individuals involved. This report presents the results of study on biometrics and privacy, performed jointly by the Data Protection Authority of the Netherlands ('Registratiekamer') and the Netherlands Organisation for Applied Scientific Research - Physics and Electronics Laboratory (TNO-FEL).

This report starts with a description how biometrics can be used for the purpose of identification and authentication. An overview of the currently available technologies is given. Next the report addresses the legal framework for the processing of personal data, as given by the European Directive 95/46/EC. From this Directive it follows that, in the context of biometrical identification, the recordings of human characteristics generally classify as personal data.

In some special cases these personal data can be classified as processed in a purely personal activity, which implies that the Directive is not further applicable. In most cases the processing is within the scope of the Directive. Some of the main consequences for biometrics are: (a) persons should know that the collection of personal data takes place (b) the data collected for a certain purpose, e.g. identification, may not be used for incompatible purposes, such as determination of health condition, emotional state or race.

Some personal data are classified as sensitive in the sense of the Directive. In the report it is argued that some human characteristics can be classified as such sensitive data. These data should adhere to a stricter regime, which is dependent on the implementation in the different member states. In some cases explicit consent of the person involved is needed, in some other cases, e.g. the central storage of templates containing sensitive data, it may be necessary to

persoonsgegevens Ten eerste zijn biometrische gegevens *persoonsgegevens*, primair omdat ze bedoeld zijn om mensen van elkaar te onderscheiden, en vallen derhalve onder de daarvoor relevante wetgeving. Op het moment geldt de Wet persoonsregistraties (Wpr) waarin de omgang met persoonsgegevens geregeld wordt. Er is een nieuwe wet in behandeling, de Wet Bescherming Persoonsgegevens (WBP). Gelet op de parlementaire behandeling is de verwachting dat deze rond de jaarwisseling in werking zal treden. De nieuwe wet is in grote lijnen gelijk aan de Europese richtlijn van 24 oktober 1995. Op hoofdlijnen kan uit de richtlijn daarom bepaald worden aan welke eisen biometrische identificatie in ieder geval moet voldoen. Bijvoorbeeld geldt het volgende algemene beginsel:

Artikel 6 van de richtlijn:
De Lid-Staten bepalen dat de persoonsgegevens:
(a) eerlijk en rechtmatig moeten worden verwerkt;
(b) voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden moeten worden verkregen en vervolgens niet worden verwerkt op een wijze die onverenigbaar is met die doeleinden.

Artikel 6(a) betekent bijvoorbeeld dat het verwerken en verzamelen van gegevens op een eerlijke manier dient te gebeuren. Mensen moeten dus weten dat er biometrische identificatie plaatsvindt. Artikel 6 (b) betekent bijvoorbeeld dat wanneer biometrische gegevens worden ingewonnen om vast te stellen of iemand bevoegd is tot toegang tot een systeem, het onverenigbaar met dat doel zou zijn als deze gegevens gebruikt worden om de emotionele toestand of het ras van de betrokkene te bepalen.

Overigens zijn er bepaalde gevallen denkbaar waarbij de richtlijn niet van toepassing is. Artikel 3 (2) van de richtlijn luidt: De bepalingen zijn niet van toepassing op de verwerking van persoonsgegevens die door een natuurlijke persoon in activiteiten met uitsluitend persoonlijke of huishoudelijke doeleinden worden verricht.

Als het dus een puur persoonlijke activiteit betreft, dan is de richtlijn niet verder van toepassing, ook al gaat het om een persoonsgegeven. In dit verband kan de authenticatiemethode van belang zijn. Zo zijn er prototypen van een flinterdunne vingerafdruklezer, ingebed in een chipkaart. Bij deze opzet komt de vingerafdruk dus noch tijdens de eerste vastlegging van de gegevens, noch tijdens de gebruiksfase buiten de kaart. De kaart geeft alleen een signaal af: de juiste persoon houdt de kaart vast, ja of nee. Het is te vergelijken met het openen van een huis met de goede sleutel. In dat geval kan gesteld worden dat de persoonsgegevens in het persoonlijke domein blijven en de richtlijn niet verder van toepassing is.

Op hoofdlijnen gelden voor verantwoord biometrie de volgende vragen:

1 Welke gegevens zijn echt nodig voor het doel?
2 Worden de gegevens rechtmatig ingewonnen? Is de betrokken persoon geïnformeerd?
3 Is er sprake van 'bijzondere gegevens'?
4 Wat gebeurt er met de oorspronkelijke biometrische gegevens? Worden deze verwijderd?
5 Zijn de biometrische gegevens zo opgeslagen dat ze niet meer terug te voeren zijn tot de oorspronkelijke gegevens?
6 Is het mogelijke om de meting van de gegevens en de verificatie decentraal te laten plaatsvinden?
7 Is de beveiliging van templates voldoende?
8 Rechtvaardigt het doel een eventuele centrale opslag van biometrische gegevens?

Conclusie

De komst van biometrische identificatie is een belangrijke trend binnen de beveiliging. Verantwoorde inzet van biometrische identificatie betekent dat rekening wordt gehouden met de wetgeving voor de bescherming van persoonsgegevens. Ook is het belangrijk dat een identificatiesystemen technisch zo worden ingericht dat een minimale hoeveelheid persoonsgegevens wordt ingewonnen, en dat de verspreiding van die gegevens voorkomen wordt.