Two barriers to realizing the benefits of biometrics

A chain perspective on biometrics, and identity fraud as biometrics' real challenge

Jan Grijpink*

ABSTRACT

Along at least twelve dimensions biometric systems might vary. We need to exploit this variety to manoeuvre biometrics into place to be able to realise its social potential. Subsequently, two perspectives on biometrics are proposed revealing that biometrics will probably be ineffective in combating identity fraud, organised crime and terrorism:

- the *value chain perspective* explains the first barrier: our strong preference for large scale biometric systems for general compulsory use. These biometric systems cause successful infringements to spread unnoticed. A biometric system will only function adequately if biometrics is indispensable for solving the dominant chain problem. Multi-chain use of biometrics takes it beyond the boundaries of good manageability.
- the *identity fraud perspective* exposes the second barrier: our traditional approach to identity verification. We focus on identity documents, neglecting the person and the situation involved. Moreover, western legal cultures have made identity verification procedures known, transparent, uniform and predictable. Thus, we have developed a blind spot to identity fraud. Biometrics provides good potential to better checking *persons*, but will probably be used to enhance identity *documents*. Biometrics will only pay off if it confronts the identity fraudster with less predictable verification processes and more risks of his identity fraud being spotted. Standardised large scale applications of biometrics for general compulsory use without countervailing measures will probably produce the reverse.

This contribution tentatively presents a few headlines for an overall biometrics strategy that could better resist identity fraud.

Keywords: biometrics, value chain, identity fraud, strategy, management, law enforcement, identity checking, identity document

1. INTRODUCTION

Biometrics is using your body as a digital key to get access to secured services and data, or using a physical characteristic to automatically recognise somebody. These days, information technology makes it possible to quickly digitise physical characteristics so that we can either depict them as an image or subject them to calculations which result in numbers, so-called biometric templates. This can be done with the contour of a hand or a finger, a fingerprint or the pattern of an iris or a retina.

1. fingerprint
2. finger geometry
3. hand geometry
4. pattern of an iris
5. vein pattern in the retina
6. face recognition
7. voice recognition
8. dynamic signature (speed and pressure while signing)
9. rhythm of typing certain words on a keyboard

Fig. 1. Examples of biometric characteristics

* J.H.A.M. Grijpink, economist and lawyer by education and information strategist by profession, is Principle Advisor at the Strategy Development Department of the Netherlands Ministry of Justice. In 1975 he obtained a postgraduate degree in management consultancy at the Stichting interacademiale opleiding organisatiekunde (SIOO) and in 1997 his Ph.D. at the Technical University of Eindhoven. He is a Certified Management Consultant (CMC) and a Registered Information Expert (RI).
j.grijpink@minjus.nl; www.keteninformatisering.nl (articles in English included)

Even variable physical characteristics can be used for biometric identification of an individual, such as his voice, the way he moves his hand when writing his signature, or his rhythm when typing certain words on a keyboard. See Fig. 1.

This contribution deals with the use of biometric data with the purpose of checking someone's identity during transactions (admission, ordering, payment, agreement) using computerised systems, on the spot and instantaneous, both for the protection of individuals and for the prevention of identity fraud and crime. Certain biometric technologies such as DNA are not (yet) suitable for this purpose, and are therefore not addressed here. The use of biometrics in criminal proceedings for the identification of mortal remains and in investigations into people's origin, descent or health also fall beyond the scope of this contribution.

Two examples illustrate the biometrics domain covered by this contribution:

Example 1

The first example is an off-line local application using an anonymous biometric template without a link to an identity document. This application is designed to prevent people from remaining in the building (e.g. a museum or a bank) after it closes. The biometric template is linked to a one-off pin code selected by the visitor himself. This pin code is necessary because the 'point of reference' of a unique chipcard number is not available in this application. The self-selected pin code indicates which templates have to be mutually compared. Without that pin code a comparison of templates is not reliable, because measurements of the same physical characteristics of the same person always show minor differences. For this reason, two measurement values that are in close proximity to each other do not necessarily originate from the same person. Because this application does not register any other information about the visitor and the one-off pin code is selected by the person himself, the visitor's anonymity is guaranteed. The application works as follows. A visitor can only enter the building once he has entered the self-selected pin code and the access computer has calculated a biometric template based on the shape of his hand, for instance. He will only be able to leave the building again once he has re-entered his pin code and the computer has not detected any major deviation between the biometric measurements related to that pin code upon his arrival and departure. The computer then deletes both the self-selected pin code and the two biometric templates. A check is made to establish whether all readings have been deleted every evening when the museum closes. If not, all visitors to the museum have not yet left the building. If a visitor is indeed found in the building after closing time, it is possible to establish whether that person is the one that the museum staff are looking for by checking with the biometric characteristic that remains in the computer.

By using an anonymous biometric detail we can electronically, without human intervention, establish that *the same* person has arrived and departed, without needing to know the exact identity of the visitor concerned. For the significance of biometrics for the protection of privacy, it is important to be aware that anonymous biometrics can be just as accurate and safe as personalised and semi-anonymous biometrics.

Example 2

This example is an application at an airport that is designed to detect suspect luggage, and to prevent people from being supplanted between the moment they check in and the moment they board the aircraft. This application makes use of personalised biometrics relating to some types of document. The application works as follows. At the moment that the passenger checks in, his biometric template is calculated and stored in a temporary file for the flight in question together with the (unique) numbers of the boarding pass and any luggage labels. When the passenger is due to board the aircraft, as part of the safety check the template is recalculated and compared with the template in the temporary file that accompanies that particular boarding pass. If the discrepancy between the measured values is too big, it is desirable to conduct a further identity check to establish whether that person has been supplanted. If the comparison shows that this is not the case, the biometric data are immediately deleted. If, at the time of departure, there is still an unmatched biometric detail left in the temporary register, the accompanying luggage can be traced and taken off the aircraft. This luggage apparently does not belong to one of the passengers who have boarded, and represents a safety risk. Because boarding passes are issued in people's names once proof of identity has been verified, this application makes use of personalised biometrics. However, if the personalised biometric data are deleted immediately after they have been used, this application of biometrics does not invade people's privacy. The advantage of personalised biometrics in this application is that in cases of doubts about someone's identity or unattended luggage, the airport staff immediately know whom they need to look for. In the event of a deliberate act, the biometric characteristic left behind can be used to prove who was involved in the incident.

Biometrics derives its significance from the person based nature of the physical characteristic that serves as the point of recognition. In comparison with the customary non-person-based methods to check someone's identity such as pin codes, passwords, electronic signature or encryption keys, biometrics therefore has a number of general advantages, which - depending on the application - make the recognition of an individual person accurate whilst simultaneously safeguarding against fraud and protecting people's privacy. Biometrics can be used to verify a person's identity even if his true identity is not or cannot be known. In these cases biometrics makes it possible to determine whether a person is the same person as the one you expect. Many social processes require exactly this and can do without knowing someone's true identity. These general advantages are however accompanied by some disadvantages. The technology is sensitive to fraud not only

with regard to the equipment, but to organisation and procedures as well. Because a biometric reading does not yield precisely the same image or template on each occasion, biometrics does not provide complete certainty. The recognition quality of a biometric application depends on appropriate parameter setting by which one can state which measurement discrepancies are acceptable to be still able to assume that the values originate from the same person. The more accurately we configure the calculation, the less chance there will be that somebody else is considered to be me, but the chance of my not being recognised increases accordingly! The advantages of biometrics over human visual checks are however of overriding importance if we want to guarantee people's privacy or if one may expect many human recognition errors in a concrete situation. For instance, if one has to check large numbers of people quickly, over a long period of time or from a distance. Neither are biometric techniques subject to recognition errors due to faulty observation resulting from preconceptions, distraction or tiredness.

This contribution presents two perspectives on biometrics to reveal how we unknowingly limit its potential social value in our information society. The result will probably be that biometrics will prove to be ineffective in combating identity fraud, organised crime or terrorism. These two perspectives are the value chain perspective and the perspective derived from the phenomenon of identity fraud.

- ✓ The *value chain perspective* explains the first barrier to realising the benefits of biometrics: our strong preference for large scale biometric systems for general use. General use of biometrics causes successful infringements to spread unnoticed. It will be argued that a biometric system will only function adequately within the boundaries of a value chain, and only if it is indispensable for solving that particular value chain's dominant problem (see reference 2 for an explanation of the theory behind the value chain perspective). In a value chain thousands of independent organisations work together to realise a social product, e.g. healthy food, less crime, faultless health care, safe travel, a value chain being a temporary co-operation between these organisations focussed on the solution of their dominant chain problem. This is a chain wide problem that puts the whole value chain product at risk, no individual chain partner being able to solve it on its own. This tie of any biometric system with its value chain means that general use of a biometric system makes it more difficult to manage and lets successful infringements unnoticeably spread (see reference 2 for an explanation of this phenomenon for a comparable identity instrument, a personal number). Only if biometric security provisions or biometric person recognition are indispensable for solving a chain's dominant problem, can that biometric system be managed adequately. As long as we underestimate the strength of the ties between tailor made biometric solutions and their value chains and focus on standardised large scale application of biometrics for general use, biometrics will not be effective in combating identity fraud, organised crime and terrorism. This perspective will be explored further in chapter 3.

- ✓ The *identity fraud perspective* exposes the second barrier to realising the benefits of biometrics: our traditional approach to identity verification. We focus on identity documents, neglecting the person and the situation involved. The latter differs from situation to situation, from value chain to value chain. This implies that the process of identity checking is rapidly becoming the main issue and the way we make use of the great variety of possible biometric applications to develop tailor-made solutions (see reference 3). With our traditional western legal-administrative approach to identity documents we unintentionally facilitate identity fraud by our pursuit of simplicity, uniformity and transparency. This has made our identity verification procedures step by step more known, transparent, uniform and predictable, enabling the identity fraudster to predict where, when, how and by whom his identity will be checked. The element of surprise is only enjoyed by the identity fraudster. Thus, we have developed a blind spot to identity fraud. Moreover, identity verification procedures are often public and can be inconspicuously observed in order to establish weak points in the technology, the organisation or the procedures. With a certain amount of preparation, an identity fraudster can outwit most identity checks (see reference 4). Biometrics will only pay off if it confronts the identity fraudster with less predictable verification processes and more risks of his identity fraud being spotted. As long as we use biometric solutions to enhance the quality of identity documents instead of the quality of the verification processes and focus on standardised large scale application of biometrics for general use *on* identity documents, biometrics will not be effective in combating identity fraud, organised crime and terrorism. This perspective will be explored in chapter 4.

But first we will explore in chapter 2 the enormous variety of biometric applications for person recognition and identity verification to understand better the way tailor made biometric solutions are able to effectively solve major chain problems, or to prevent identity fraud.

Biometrics provides both protection against crime and against intrusion on one's privacy. The public interest in biometrics is growing and the technology is making rapid progress. An information society needs identity checking using person related characteristics. Therefore, biometrics can be expected to play an important role in the long term. Because the development of new technology usually goes through bad patches, a well considered strategy is necessary for the application of biometrics. Such a strategy should be based on the insights that diversified use of biometrics in a number of important value chains determines whether biometrics will live up to its promises of security and safety and privacy protection and that biometrics can only prevent identity fraud to happen, if it is used to improve the identity checking process in a specific situational context instead of simply adding to the features of an identity document only.

2. THE VARIETY OF BIOMETRIC SYSTEMS FOR TAILOR-MADE SOLUTIONS

This chapter explains the enormous variety of possible biometric solutions, using a number of features and aspects of biometrics that can be combined in various ways to realise different designs.

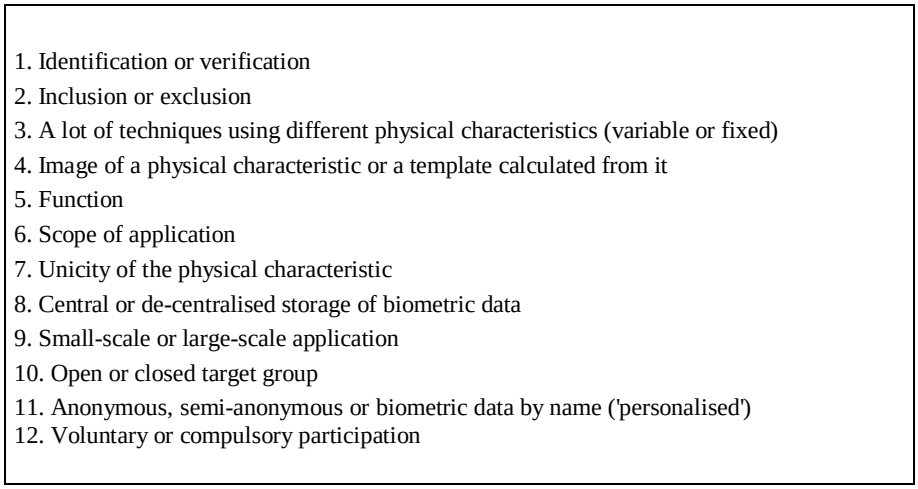

Fig. 2. Features of biometric systems

Biometrics calls for tailor-made solutions, no single biometric technique nor form of application is suitable for every problem relating to identity checking. This is important because we need different tailor-made solutions for different dominant chain problems and we need to prevent identity fraud by a large number of small-scale, sector-restricted applications. These offer a double advantage to the protection of privacy and the prevention of crime: one can reduce the consequences of an identity fraud that has not been detected to a minimum, and subsequently have more opportunities to unmask a successful impostor. In addition, sector-restricted applications offer more legal protection against unlimited linking of personal details using biometric templates. Within a small-scale application the voluntary use of biometrics can be more easily handled because non-biometric exceptions for people who really object to this method of checking one's identity can be better controlled. Fig. 2. gives a picture of twelve different features of biometric applications that can be used to realise tailor-made solutions. The list is not meant to be exhaustive.

A. Identification method

The implications of biometrically checking people's identities for their privacy and protection against fraud is significantly determined by the method used for the recognition of an individual. We make two different distinctions:

1. Identification or verification

This distinction relates to the envisaged knowledge of a person's identity.
There are two alternatives:

a) establishing precisely *who* someone is (identification);
b) establishing whether a person is *the same* person as expected (verification).

The establishment of a person's true identity involves a thorough investigation into someone's identity, which is rarely done in the Netherlands outside of criminal law enforcement and immigration. It is deemed sufficient to establish

whether a person is the same person as expected, by ascertaining whether several pieces of information belong to the same person, for example. Verification is less far-reaching than identification because we remain unsure whether a person actually is *who* he says he is. But in many social situations this is sufficient.

2. Inclusion or exclusion

This distinction between inclusion and exclusion relates to another basic approach to checking someone's identity:

a) we can *positively* establish whether someone is indeed the right person.
   This is referred to as the 'inclusive' use of a recognition technique;
b) we can *negatively* establish that someone is *not* the right person.
   This is referred to as the 'exclusive' use of a recognition technique.

A single point of difference is sufficient to exclude someone with one hundred percent certainty! On the other hand, inclusive use *never* gives one hundred percent certainty, even though that certainty does of course grow with each point of similarity that is ascertained. When using only one biometric template, it is only possible to perform an 'inclusive' check. If it is necessary to establish immediately that someone is *not* the right person (exclusion), at least two different biometric characteristics have to be used. After all, in a case of mistaken identity, the chance of two physical characteristics being relatively just as close together is virtually ruled out.

The 'exclusive' use of a biometric characteristic to establish that someone is *not* the same person barely penetrates into people's private lives, but inclusively establishing a person's identity does. Information technology does in fact make the least radical form of checking someone's identity biometrically, the *exclusive* use of *anonymous* biometrics, technically feasible. Therefore, from a privacy perspective it is notable that most people unnecessarily show a spontaneous preference for the most radical form, the *inclusive* use of *personalised* biometrics.

B. Biometric technique

3. A lot of techniques using different physical characteristics (variable or fixed)

Fixed physical characteristics can be more successfully imitated than variable characteristics. A person can also himself change a variable physical characteristic without this being noticed. This is useful if a person is under threat, but will generally fail to offer an adequate solution for situations in which it pays to pass oneself off as two different people. If considerable advantage can be gained by doing this, it is better to use an unchangeable physical characteristic.

4. Image of a physical characteristic or a template calculated from it

With an image of someone else's finger tip, a person can pass himself off as someone else when checked, for instance to spuriously suggest this person's involvement in a transaction or action. These situations can not as easily occur if use is made of a template. This is a biometric number calculated from unique features found in a fingerprint, for instance. Because the other information contained in the image is not used in the calculation, it is not possible to retrospectively calculate the original image of the fingerprint from the biometric number (template). There are countries that (want to) forbid the central storage of biometric *images*, or impose stricter regulations on the central storage of biometric images than will apply to the central storage of *templates*.

C. Implementation

5. Function

Biometric images or templates fulfil all sorts of functions, often several at the same time. The ability to recognise a person as the right one is in itself an important function, but using a biometric characteristic one can also establish that two details belong to each other, e.g. for verification purposes. Linking or checking personal details with a biometric characteristic related to that particular person is more reliable than with any other not person related given such as a number, a word (name) or an image (photograph, signature or logo). Comparing details with biometrics can prevent or reveal errors. The biometric detail can prevent confusion if other identifying personal details are not unique, for instance if a foreign name can be spelled in more than one way. In combination with other data, biometrics enhance the ability to manage databases and combat data contamination or fraud. It is important in this context that one can check whether somebody wrongly has more than one identity at his disposal or that an identity is wrongly being used by more than one person.

6. Scope of application

Biometric systems have a certain scope of application, in terms of both content and geographical area. Some are only used within a specific sector or value chain (examples are the use of biometrics in the health service or in the penal law enforcement chain). Other systems are more general, because they are used in several sectors or chains. Biometric systems can be local (e.g. a biometric system for building access), regional, national or international. An example of the last category of biometric systems is a biometric passport.

7. Unicity of the physical characteristic

The unicity of a physical chracteristic has apart from a physical dimension two additional ones: time and place. Generally, a fingerprint is regarded as unique, although some races have fingerprints with cannot be measured because the relief is too low. The uniqueness of many other physical characteristics is uncertain. Fortunately, absolute uniqueness is not a prerequisite for every application of biometrics. If the target group is relatively small or if the person is expected back at the checkpoint within a short period of time after first admission, the use of a less than unique characteristic can result in an accurate person recognition.

8. Central or de-centralised storage of biometric data

At the one extreme, there is the decentralised storage of a single biometric detail on a single chipcard placed in the hands of the person from whom the biometric detail originates. The other extreme consists of the storage of all biometric data in a central file for on-line checking without the use of a chipcard. The biometric details can be physically concentrated at the same location, but this is not necessary, 'central' in this context means that all stored biometric details can be directly accessed and compared with each other. This makes it possible to establish, for example, whether a person is already included in the file, but under a different name.

9. Small-scale or large-scale application

In a small-scale application, the uniqueness of the physical characteristic is less important because the chance of two individuals having virtually the same physical characteristic reduces significantly as the target group becomes smaller. In large-scale applications deliberately passing oneself off as someone else tends to be more successful and more valuable. This is not so much due to the technique itself as to the number of people, the vast organisation and extensive procedures involved. Small-scale applications are less risky and tend to increase privacy, particularly if the applications make use of different biometric techniques. This way one can also limit the damage of an undetected identity fraud.

10. Open or closed target group

A closed target group is one in which every member is known beforehand. In a closed group the chance of two virtually identical measurements that could possibly lead to mistaking a person's identity is smaller than with open target groups. Within closed groups a simple application using anonymous biometrics yields a check in which an outsider has very little chance of successfully passing himself off as one of the members of the group.

*11. Anonymous, semi-anonymous or biometric data by na*me ('personalised')

If biometric data can only be traced back to the person from whom the measured value originated with disproportionate effort, the biometric data are anonymous data and cannot be regarded as personal data. A good example of anonymous biometrics is dirty glassware in a restaurant. It is a hopeless task to trace a fingerprint on one of the glasses to a restaurant diner who has already left. One will never be able to find him. This could explain why we don't concern ourselves too much with this glassware in practice. To assess the possibilities to find the person from whom a biometric given originates, we have to look at the application as a whole rather than only at the biometric detail on its own. The situation is different when it comes to personalised biometrics, in which case the biometric detail is attributed to a specific person referred to by name, or the name can be established with some - but not disproportionate - effort. Semi-anonymous are biometric data of which only one party (person, organisation) knows from whom the biometric characteristic originates, e.g. the issuer of a biometric chipcard. Other parties do not. In their eyes the biometric data are anonymous. With a semi-anonymous biometric chipcard one's identity can only be checked anonymously by other parties, thus accurately establishing that the cardholder is the right person without knowing who he is.

12. Voluntary or compulsory

Compulsory use of biometrics by the government or by private bodies requires a legal basis. In the European Union the voluntary use of personalised biometrics is in principle permitted, unless the biometric characteristic can be used to establish someone's race or origin. But is voluntary co-operation always truly voluntary? This is not solely determined by market conditions, but also by the existence of a fully-fledged alternative facility without biometrics, so that true freedom of choice is possible. If on a really voluntary basis, even a public authority may use biometrics without such use being explicitly provided for by the law.

These twelve aspects illustrate that the design of a biometric application involves a large number of implicit choices that determine the effectiveness of the application, its sensitivity to fraud and its consequences for personal safety and security. A wide range of different applications is possible. If applied on a large scale, most biometric techniques are vulnerable to fraud and privacy breaches currently. It is important to bear in mind that - unlike the situation in the analogue era - it is not the verifier but the person being verified who has the upper hand. After all, he is one hundred per cent certain of being able to activate an emergency procedure, by imperceptibly using someone else's chipcard, for example, or by pretending that he has lost his card. Therefore, from the perspective of protecting people's privacy and security in an infor-

mation society, anonymous and semi-anonymous biometric applications in particular will in the future have major significance. 'Anonymous' meaning that it is not reasonably possible to establish who somebody is, 'semi-anonymous' that nobody can find out who you are with the exception of a trusted party, e.g. the issuing authority of an identity instrument. Small, 'exclusive', (semi-)anonymous biometric systems, combining the identification methods of exclusion ('that is not him') and verification ('he is the same person, but I don't know who he is'), are very promising for a safe and free information society especially if the target group can be considered to be a closed group. In these cases even simple technology and procedures are sufficient. Biometrics will not realise its full social significance until we recognise and utilise the wide-ranging possibilities offered by the anonymous or semi-anonymous use of biometrics.

3. A VALUE CHAIN PERSPECTIVE ON BIOMETRICS

In this chapter a value chain perspective on biometrics is presented consisting of three principles:

a) A dynamic chain concept based on a dominant chain problem as the trigger of temporary chain co-operation;
b) The role of this dominant chain problem within the irrational context of a value chain;
c) A multi-level focus on a value chain.

a) A dynamic chain concept based on a dominant chain problem as the trigger of temporary chain co-operation

A value chain can be seen as a temporary pattern of co-operation around a dominant chain problem. A dominant chain problem is a recurring operational problem that is vehemently felt in every link of a value chain, no chain partner being able to adequately tackle this problem on his own. Solving this recurring operational problem is exactly what brings about the structural collaboration between the parties involved. As soon as the dominant chain problem fades away or shifts towards a different problem, the value chain re-arranges itself to better cope with the new dominant chain problem. This idea of a shifting chain problem implies a rather unusual dynamic concept of a value chain. However, it can better explain the peculiar dynamics of more complex social value chains, such as the chain co-operation in the stockbreeding chain to make sure that the meat is of no threat to your health or in the asylum chain to guarantee that undocumented asylum seekers can only have *one* new identity (henceforth the 'right' one!) in the European Union.

b) The role of this dominant chain problem within an irrational context

The second component of our chain perspective is the absence of an all-encompassing authority in a value chain which causes a decision-making process at the chain level to be poorly organised and irrational. Problems and solutions are randomly connected in a decision-making process that is only partly known or ambiguous. This randomly connectedness is meant by 'irrational'. The chain partners repeatedly find themselves placed in unexpected situations. As long as a specific dominant chain problem is keeping the chain firmly in its grip, this chain problem functions as the real 'boss' in the value chain. As soon as this dominant chain problem loses its impact, the chain resolves itself or regroups around a new dominant chain problem. This idea of an irrational chain environment is useful to biometric systems, because it implies that a biometric system depends on the ups and downs of the dominant chain problem requiring biometrics to be adequately solved. Only as long as the dominant chain problem really triggers the co-operation within this value chain, can the quality of its biometric system be counted on.

c) Multi-level focus on a value chain

The third underlying principle of the presented chain perspective consists of a multi-level focus on chains. Fig. 3 visualises this multi-level focus illustrating how biometric systems can be positioned at three levels with regard to a specific value chain: (1) at the 'base' of a value chain, (2) at a collective level within the boundaries of a value chain, to be indicated by 'chain level' and (3) at a general supra-chain level above several value chains.

A biometric system at the 'base' of a value chain refers to an organisation's internal biometric system, for instance to control access to a vulnerable building or installation. These biometric systems can also be used by one or more partners in the chain in their bilateral communication. Chain biometrics, on the other hand, forms part of the information infrastructure of a value chain and can be seen as positioned at 'chain level'. This means that the biometric system is managed collectively by or on behalf of all organisations in the value chain, i.e. independently of individual chain partners. Chain biometrics supports and steers the exchange of information between collaborating organisations in the chain from the collective 'chain level'. General biometric systems are positioned at a level above several value chains to be used by organisations in these chains, with different functions and patterns of use in each of these chains. Thus, general biometric systems are not chain-related.

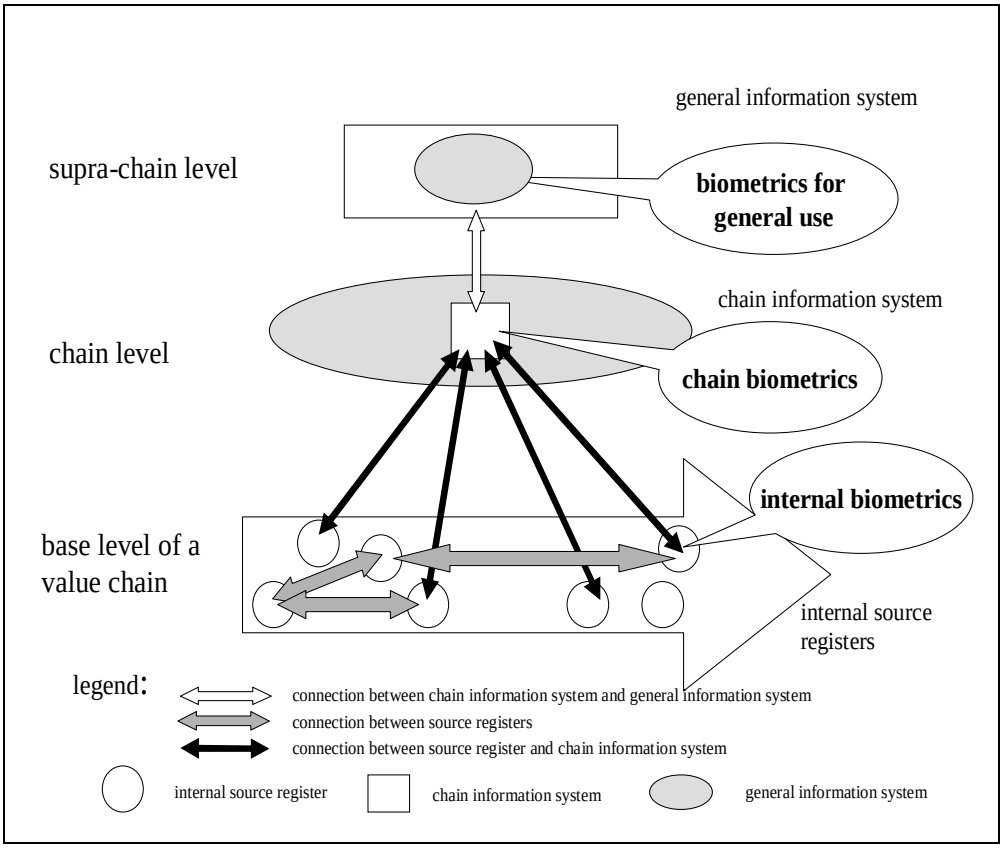

Fig. 3. Biometric systems at three levels with regard to value chains

Chain biometrics

A biometric system must primarily be up to its function in a specific value chain. This, after all, is what determines the requirements for the biometric application and the volume of fraud that could threaten the correct functioning of the chain. A short distance between chain biometrics and its dominant chain problem yields a wide range of chain-related, self-cleaning mechanisms. Those mechanisms work best when the biometric system is absolutely indispensable for resolving the dominant chain problem. Only then will the biometric system maintain itself for a longer period of time at chain level. If an existing chain biometric system is no longer necessary to solve this chain's particular chain problem, the chain partners are no longer motivated to properly manage their biometric system together and actively monitor it against misuse and fraud. It then 'sinks' to the base level of a chain for internal use, if it is kept alive at all. The starting point for a biometrics strategy is therefore that a stable biometric system is intrinsically tied to a value chain. This system can only be stable as a chain biometric system if tied to a dominant chain problem that cannot do without it.

Supra-chain biometrics

Supra-chain biometrics is chracterised by multi-chain use of the same biometric system. Such biometric systems are more difficult to manage and more vulnerable to contamination and fraud. Because biometrics is still in an early stage of development, this point can best be explained with a concrete and topical example from a related phenomenon, personal number systems: the Dutch social security number. Up until the middle of the nineteen-eighties, the (original) tax number was only used internally by the Dutch tax authorities. It was not given out to other authorities nor used by employers. Since 1985 it has been a public number, and since 1988 it has also been used by the social security sector, re-christened as the social security number. In this sector the social security number began to function as a framework for registering, accessing and linking details about work, social security premiums, benefits and facilities. It was not legally permitted to use the social security number outside of those two sectors. That changed in the middle of the nineties; a start was made in 1996 with placing the social security number on the passport and driving licence, two important Dutch ID documents. A wide range of bodies, both within and outside of the public sector, can now legally take it over from an ID document that has been presented to them and use it (internally). In 2001 the social security number was legally designated as the

education number for the verification of the financing of schools and other applications in the education area. Finally, a political decision is expected in the near future regarding the question of whether the social security number (possibly in encrypted form) will also be used in the healthcare sector as a unique care identification number (CIN). Using the CIN for access purposes to medical files, it will eventually be possible to put in place a virtual patient file for all. Fig. 4 summarises the gradual development of the social security number: from confidential internal number, through increasing multichain use to one of the current candidates for a compulsory general personal number. It can be assumed that biometric systems in future will show similar growth patterns as personal numbers.

Ministry	Application	Notes
Finance	tax liability, tax payment	confidential fiscal number until 1985, public thereafter
Social Affairs & Employment	registration of employment, social security premiums, benefits and facilities	since 1988 also used by the social security sector.
Home Affairs	identity (social security number on passport and driving licence)	since 1996 also used by the identity chain
Education, Science & Culture	financing schools and other applications	since 2001 also used by the education sector
Health, Welfare & Sports	medical patient file	will perhaps also be used by the healthcare sector in the future

Fig. 4. Development of the Dutch social security number

Why do we tend to opt for a general supra-chain biometric system even if we accept its natural ties with a value chain? Firstly, we underestimate the costs of sharing a biometric system like it has been for personal numbers. People often do not have a clear picture in mind of the increasing management problem and costs because of the multi-chain use. After all, a general supra-chain system plays a different role in each of the chains that are using it. In each chain it is affected by chain-specific sources of contamination and forms of fraud. In the case of multi-chain use, this leads to unexpected management problems because people in the one chain have no idea about the specific contamination sources and forms of fraud in other chains that are making use of the supra-chain system. Multi-chain use increases the value of the supra-chain biometric detail, which makes abusing it more attractive. Moreover, supra-chain biometric systems are less easy to gear up to the diverse requirements of various chains that make use of the system. This is why supra-chain biometric systems are basically more difficult to manage without the cleaning mechanisms triggered by an unambiguously focussed collaboration and enforced by the whip of its dominant chain problem. The requirements from various chains can be very diverse, making it worth while to examine which forms of management are available for a biometric system.

In Fig. 5. a distinction is made horizontally between passive and active management, and the scope of the management activities is given vertically, from issuing a biometric instrument to monitoring its use. This gives rise to six different management forms for biometric systems. Depending on the application and value of the biometric detail, every chain features some general and some chain-specific sources of contamination and forms of fraud. A biometrics administrator can prepare himself for this by making use of all chain-related self-cleaning mechanisms. Generally speaking, people will therefore opt for the simplest and cheapest management form that meets the requirements. Management form 1, for example, is usually adequate for temporary chain biometrics that represents no real threat to the enrolled persons, whereas management form 6 is more appropriate for the management of a permanent public biometric system with a substantial social value and a serious personal risk, e.g. the access to virtual medical files. Multi-chain usage yields a different picture, if the chains set different requirements for the same biometric system and – accordingly – its management. The requirements of the most vulnerable chain should be applied to a supra-chain biometric system, but there is usually a lack of support for the costs of a high security management variant in chains which themselves set less strict requirements.

	Passive	Active
Issuing	1 enrollment on request without ID check	2 enrollment with legally prescribed ID check based on documents and other data
Administration	3 registering holders' details	4 registering holders' details, and periodic check of the holder's rights to prevent misuse
Monitoring	5 registering details about the use of the biometric detail and registering misuse or attempts at misuse	6 registering details about the use and registering misuse or attempts at misuse, and combating misuse, before and after

Fig. 5. Six management forms for biometric systems

The starting point for a biometrics strategy is therefore that a stable biometric system is tied to a value chain, functioning well at chain level as long as the biometric system is indispensable for solving that particular value chain's dominant problem. Indeed, supra-chain biometrics can sometimes be effective and stable, but this will only be the case if the biometric system is embedded in chain specific control systems geared to their own requirements. A socially robust biometrics strategy should therefore be based on the insight that biometric systems are principally chain-tied and chain-specific, and that multi-chain use of a biometric system generally makes a supra-chain biometric system unstable, difficult to manage and vulnerable to contamination and fraud.

In the end, biometrics will undoubtedly be indispensable for person recognition and identity checks in our information society. But biometrics will only be up to this mission if we develop a great variety of tailor-made biometric systems and pay much attention to their management and use. Administrators and politicians must get accustomed to the idea that a complex information society needs a biometrics strategy with a multitude of high quality biometric systems. Chain bound biometrics in a great variety of tailor-made solutions will be one of the pillars of the future information society. Effective combating of identity fraud and misuse of biometric images and templates will decide on our safety and privacy in an information society.

4. IDENTITY FRAUD AS BIOMETRICS' MAJOR CHALLENGE

All over the world, in countries with highly different legal cultures, a great deal of effort is being spent improving the identity management and tightening up the policy governing identity verification in order to enhance security. Countries without or with only limited compulsory identification such as the Netherlands are now introducing a general compulsory identification. Countries without laws for general compulsory proof of identity, such as the United Kingdom, are now taking steps to introduce this identity instrument. Moreover, many countries are giving consideration to adding a biometric feature of the holder to identity cards and travel documents. The purpose of a more stringent identity policy is to enable the establishment of someone's identity or the verification that the person involved is the right one in increasingly more situations and with greater reliability. The importance of the distinction between these two forms of identity check is that verifying that someone is the right person doesn't necessarily require knowledge of who he is. Even if the events of September 11 2001 had not taken place, this aim would still have gained more importance in keeping with the growing number of transactions that are conducted electronically and at a distance without social control or visual supervision. Electronic communication spans the whole world and in the coming years gains extra dimensions through the increasing mobility and anonymity of society. Identity checks, too, are more and more likely to be performed electronically and at a distance. This is why we will need a broad arsenal of identity instruments for person recognition and identity verification in the future. In addition to what we already have, such as electronically readable identity cards, pass numbers, personal numbers, pin codes and passwords, this will also have to include functions such as electronic signatures and biometrics.

In the western world the identity policy concentrates mainly on combating document fraud: the use of counterfeited legal identity documents. The fraudulent use of a valid identity document officially belonging to someone closely resembling the user (so called lookalike fraud) is already compelling us to face up to the problem of identity fraud. This means that somebody with dishonest intentions deliberately passes himself off under an identity that does not belong to him by using

the identity of someone else or a fictitious identity. Contrary to the current concept of identity fraud being the misuse of an identity document, identity fraud in our definition doesn't necessarily require the use of an identity document. The identity fraudster can make use of personal numbers, photos, actions or occurrences as well, because they all feature an identity suggestion from which people draw conclusions about whom they are dealing with. Therefore, identity fraud can take place anywhere and in many ways and is not restricted to specific situations, procedures or documents. Once a person has fraudulently succeeded in being accepted as someone else, he can use this 'identity' in other situations along regular channels. In these situations it usually is no longer possible to see through the preceding fraudulent identity change. Identity fraud is often the first step towards a subsequent fraud, such as a bank fraud, a passport fraud or a benefit fraud. But these more specific fraud labels distract our attention from the common denominator of these forms of fraud, which is that a cunning method is used to deliberately misuse the identity of an existing or fictitious person. When an identity fraud is successful the fraudster hides behind the other identity with all indications leading towards the victim, if there is one, and not to the fraudster. Thus, a police investigation of a successful identity fraud remains often without results.

Identity fraud as defined here, is forcing us to take a fresh look at identity instruments in our legal culture. It generally turns out that measures and instruments that are useful in combating document fraud do not provide solutions to combating identity fraud. Often they even have the reverse effect. Giving the social security number on the Dutch passport is an example to illustrate this. Since this measure was introduced in 1996 it has provoked an enormous and still growing volume of identity fraud. This identity measure was intended to make it easier for employers to know someone's social security number for various administrative purposes using identity documents for name-number verification. This name-number verification is effective if the identity document is sound and the holder is the right person. But that is no longer the case if it is used by someone else who closely resembles the rightful holder. After all, one should realise that a name-number verification with an identity document always succeeds, regardless of who is making use of the document. A look-alike person, who holds an identity document belonging to someone else, can assume that identity without being noticed and thus have a free ride with that person's social security number. Furthermore, there are many verification situations in which one is asked to hand over a copy of an identity document. Any copy can easily be adapted for use by somebody else. Giving the social security number in identity documents (e.g. the Dutch passport and driving licence) therefore inadvertently makes identity fraud much easier by handing over to the fraudster the correct number together with all the identifying personal details that belong to the rightful holder of the security number. The parallel with a biometric detail is obvious. If an identity fraudster is able to find out the measurement value or image with which his biometric details will be compared, there are many deceitful ways of misleading the automatic identity check. This example underlines the need to test all existing identity measures for their effectiveness in combating identity fraud.

This example of the social security number on identity documents illustrates also that an identity fraudster is facilitated by our western legal culture which requires regulations if public bodies enter the private domain of the civilian. These regulations unintentionally enable him to predict where, when, how and by whom his identity will be checked. Moreover, identity verification procedures are often public and can be inconspicuously observed in order to establish weak points in the technology, the organisation or the procedures. With a certain amount of preparation, an identity fraudster can outwit most identity checks. Our legal-administrative approach has made the process of identity checking step by step more transparent, uniform and predictable to the benefit of the identity fraudster. We ought to de-ritualise identity checks by making them more varied and less predictable.

Two underlying principles hinder us as well when it comes to detecting or combating identity fraud:

- ✓ Every identity card, personal number, PIN or biometric detail provides identity suggestions, which causes people to assume they know whom they are dealing with. We spontaneously trust these administrative identities, even though they are often based on unverified or unverifiable personal details. While checking someone's identity we thus tend to look at the identity document or personal number without independently screening its identity suggestion. This also applies to a biometric device: it can only compare the presented biometric detail with an earlier measurement stored on a data carrier or database, taking for granted the identity suggested by the accompanying identifying personal data. While issuing an identity document or personal number or enrolling someone into a biometric system whether it is inside or outside of the government, we unknowingly derive incorrect details from source documents, because we are not able to verify the integrity or authenticity of the document and its true relation to the person presenting it. In many cases, an information infrastructure designed to block an identity document or a personal number against use by others against the will of the rightful holder does not exist or may not be used. That is why identity fraud usually suc-

ceeds, by way of simply accepting the suggested identity of a personal card, a personal number and, in the future, that of a biometric template. This includes a cunningly cajoled admission to a sloppy fall back procedure that enables the fraudster to casually present pass for somebody else. Often the resulting authorisation can no longer be seen through during later phases of the process.

- ✓ When checking someone's identity we spontaneously ask the question 'who are you', whereas it is usually sufficient to know for sure that someone is the right person, regardless of who he is. Using a biometric characteristic, for example, somebody can be accurately identified as the right person even if we cannot find out who he is. Carefully and independently managed private and public pseudonyms such as personal numbers, pin codes, passwords, electronic signatures or biometric details facilitate all sorts of accurate identity verifications. We often leave these opportunities unused by this unnecessary emphasis on 'identity' that causes us to forget that anonymous and semi-anonymous identity checks are also possible.

Unfortunately, these two attitudes, which are inadequate for detecting or combating identity fraud, are mutually reinforcing. They explain why we spontaneously take identity measures that unintentionally increase rather than reduce the opportunities to commit identity fraud. Tightening up the prevailing identity policy will play into the hands of the identity fraudster. The most important consequence of the approach to the September 11 problem will therefore probably be that, despite all our good intentions, identity fraud will increase in scope and seriousness.

Combating identity fraud means a different way of thinking and also requires a turnaround in our approach to identity checking. Our attention should shift from the identity document towards:

- ✓ *the **person** using it*. The quality of the document is not unimportant, but not anymore the main issue in combating identity fraud. A persons' identity can also be checked by other personal details than those mentioned on the identity document. These details can come from anywhere as long as they aren't predictable or known. This can legitimately and efficiently be done in an automated way following the approach, which I have described in my publications about value chain computerisation (see ref 1). If we only have the personal details given in the identity document at our disposal, how can we actually discover that somebody isn't the legitimate holder of that identity document? It is precisely those personal details that have enabled the identity fraudster to come up with a plausible story in the first place;
- ✓ the ***process** of identity checking*. Every situation of identity checking is different, depending on the context of the checking process. In each situation, a successful identity fraud has a different social and economic value, identity checking requires different personal details and chances to prevent identity fraud differ enormously. Thus, identity-checking procedures are to be tailor-made. Predictable standard procedures undermine the effectiveness of any identity checking process. The biggest leverage affect can be expected from elements of surprise built into a varied system of private and public identity verifications;
- ✓ *suitable **checking details*** from independent sources that are not controlled by the person being checked or only known to the rightful holder of the identity document, personal number or biometric detail;
- ✓ *the **value** of an identity instrument*. Supra-chain use and mentioning of general personal numbers or biometric details give an enormous social and economic value to poorly managed identity instruments that can be easily misused by unauthorised persons. We must find ways to stop this creeping process of adding more value to less identity instruments unless counter-acted by chain-bound biometrics, tokens, personal numbers or PIN-codes and by making use of other public bodies' data.

5. AN OVERALL STRATEGY FOR IDENTITY FRAUD RESISTANT BIOMETRICS

Let us try, by way of conclusion, to formulate some headlines of an overall strategy for identity fraud resistant biometrics, making use of the inherent variety of biometric systems and the two proposed perspectives on biometrics, the value chain and the prevention of identity fraud.

1) A wide range of different biometric systems is possible and should give rise to tailor-made application of biometrics. Twelve aspects of any biometric application imply choices that determine the effectiveness of the application, its sensitivity to fraud and its consequences for personal safety and security. Biometrics will not realise its full social potential until we recognise and utilise the wide-ranging possibilities offered by the anonymous or semi-anonymous use of biometrics.
2) A socially robust biometrics strategy should be based on the insight that biometric systems are basically chain-tied and chain-specific, and that multi-chain use of a biometric system makes this supra-chain biometric system

unstable, difficult to manage and vulnerable to contamination and fraud. Supra-chain biometrics can be effective and stable only if embedded in many different chain-bound and chain-specific control systems geared to its own requirements, with inter-chain comparison of the results to detect identity fraud and to prevent the effects of succesful identity fraud from spreading from one chain to another. Effective combating of identity fraud and misuse of biometric images and templates will play an important role in keeping up our safety and privacy in an information society.

3) Identity fraud as defined here, is forcing us to take a fresh look at biometric identity instruments and the use of biometrics in the context of a specific process of identity checking, understanding the relevant legal culture. In our western world, it generally turns out that identity measures and instruments that are useful in combating document fraud do not provide solutions to combating identity fraud. Often they even have the reverse effect. Combating identity fraud means a different way of thinking and also requires a turnaround in our approach to identity checking. Our attention should shift from the identity document towards:
   - *the person using it;*
   - *the process of identity checking;*
   - *suitable checking details;*
   - *the value of an identity instrument.*

Identity checks will never be waterproof. Therefore one needs more than only one identity instrument, e.g. a biometric detail. The use of other data can strengthen the prevention of identity fraud on condition that the person to be checked has no control of its content and the procedure will not be predictable. Identity policy directed at combating identity fraud doesn't influence the need for better combating document fraud. It adds to identity policy an extra, new perspective and different solutions. If identity instruments prove to be weakening the overall identity policy, then choices between different solutions have to be made. This might be the case when a biometric detail will be given on identity documents in such a way that an identity fraudster can read or use it. This is not to say that we should be reluctant to implement a biometric system in places where it adds value in terms of protection of privacy or prevention of identity fraud. However, we should be more aware of the barriers that keep us from benefiting from biometrics. Biometrics can be expected to play an important role in an information society. Because the development of new technology usually goes through bad patches, a well considered strategy is necessary for the application of biometrics. This strategy must be in place before identity fraud is growing in number and negative effect, as we expect at the moment. Then biometrics will move towards its finest hour, but only if biometric data are reliable and biometrics confronts the identity fraudster with less predictable verification processes and more risks of his identity fraud being spotted.

Thus, this contribution presents three major insights. Be aware of the fact that biometrics will only function well within the boundaries of a value chain that cannot do without it to solve this particular chain's dominant chain problem. Do not opt for standardised large scale applications of biometrics for general use without countervailing measures, because it is not possible to safeguard such a biometric application from identity theft, fraud and privacy infringements. Design the use of biometrics to enhance verification processes with tailor-made solutions, instead of the current approach of enhancing identity documents with a standardised solution.

REFERENCES

1. J.H.A.M. Grijpink, "Chain-computerisation for interorganisational policy implementation" and "Chain-computerisation for better privacy protection", in: *Information Infrastructures & Policy* 6 (1997-1999), IOS Press, Amsterdam, March 2000.
2. J.H.A.M. Grijpink, "Personal numbers and identity fraud, number strategies for security and privacy in an information society", Part I en II, in: *Computer Law and Security Report*, vol. 18 (5 en 6) 2002, pp.327-332 en pp. 387-395, Elsevier Science Ltd, Oxford, UK , ISSN 02673649.
3. J.H.A.M. Grijpink, "Biometrics and Privacy", in: *Computer Law and Security Report*, May/June 2001, vol. 17 (3) 2001, pp. 154-160, Elsevier Science Ltd, Oxford, UK, ISSN 02673649.
4. J.H.A.M. Grijpink, "Identity fraud as a challenge to the constitutional state", in: *Computer Law and Security Report*, January/February 2004, vol. 20 (1) 2004, Elsevier Science Ltd, Oxford, UK, ISSN 02673649.