RISKS AND THREATS

Attached to the application of

BIOMETRIC TECHNOLOGY

In

NATIONAL IDENTITY MANAGEMENT

Elisabeth de Leeuw - Lecoeur

Thesis submitted in fulfilment of the requirements
For the degree of Master of Security in Information Technology
At the TIAS Business School
Eindhoven and Tilburg

AMSTERDAM, OCTOBER 2004

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

I - INTRODUCTION

CHAPTER 1 – BACKGROUND

THE ROLE OF NATIONAL IDENTITY MANAGEMENT

It is in the interest of national states, to know who its citizens are and to manage and administer the rights of foreigners to stay within its borders. Without this knowledge, national states are unable to control the flows of people moving to and from the country.

If we don't know, as a national state, whom we are dealing with, we can neither judge whether the rights claimed by an individual are legitimate, nor can we enforce laws and regulations upon individuals. Thus, in order to fight international crime, national states need to manage and administer its citizens and the flows of people moving into the country.

Due to the globalisation and mobility, international crime increases and takes new shapes. Thus, the importance of a reliable and robust national identity management increases. The issue of identification and authorisation is to be put on top of the agenda.

National identity management aims to administer the citizens of the state and the rights of foreigners to stay within its borders. The issuing of identity documents and travel documents has been a major task from the outset of national identity management. Frauds however manage to forge these documents. Many improvements have been made in order to protect documents from being forged. Consequently, fraud is shifting from *document fraud* to other types of *identity fraud*. Look alike fraud, in which case frauds use identity documents belonging to some look alike, in particular poses a serious problem. The application of biometrics might help to fight this type of fraud and thus help to improve the quality of national identity management.

AN APPROACH TO POLICIES ON NATIONAL IDENTITY MANAGEMENT

The current discussion on the application of biometrics in national identity management takes place on a tactical level. A couple of assumptions are constitutive for the discussion:
- biometrics will improve the quality of national identity management; and
- the introduction of biometrics will not fundamentally change the national identity infrastructure.

As a policy maker, I will evaluate the proposals for the introduction of biometrics not only on a tactical, but also on a strategic level. Not only am I supposed to react to the proposals on a tactical level, I also have to develop a strategy. In order to do so, it is insufficient to take the above assumptions for granted: a strategic exploration is necessary.

CHAPTER 2 – INTERNATIONAL AND NATIONAL PROPOSALS

INTERNATIONAL PROPOSALS

The following international plans are available:
- The International Civil Aviation Organisation (ICAO)
- United States plan
- European Community plan
- Dutch plans

The International Civil Aviation Organisation (ICAO)

ICAO issues standards in the field of travel documents. ICAO is a branch of the United Nations and is responsible for the promotion of security of international aviation through the establishment international agreements and standards for the facilitation of border crossing of passengers.

Due to the reputation of ICAO, the recommendations and standards are accepted by the member states of the United Nations, The Netherlands included.

In the 'Resolution of New Orleans', ICAO recommends:
1 Face as a primary, mandatory biometric feature
2 Fingerprint and iris as secondary, optional biometric features
3 Storage of the biometric feature in the shape of a digital image, mandatory
4 Storage of the biometric feature on a contactless chip on the travel document

Face, fingerprint and iris are hereditary and to a certain extent randotypic[1] physical features and therefore in principle feasible for biometric applications.

In order to make infrastructures compatible, ICAO prescribes the following infrastructure:

Sensor	To capture a biometric feature
Feature extraction unit	To extract a biometric feature
Matcher	To match (extracted) biometric features

Explanation:

To capture a biometric feature means to take a picture of it: a photograph of the face or iris or a print of the finger. In this context, an electronic picture is taken.

To extract a biometric feature means to take a subset of the data of the electronic picture, according to predefined standards, in order to prepare the data for electronic processing. A fingerprint for example might be too wide; a picture of a face might include the neck.

To match biometric features means that a biometric feature extracted from a living subject is compared to a stored biometric feature. The stored biometric feature is in fact also an extracted of the original picture.

[1] See Table 3 for an explanation of genotypic, randotypic and behavioural biometric features

United States

The United States accepts the recommendations and standards established by ICAO. Within this framework, the US prescribes
1. Face as a primary, mandatory biometric feature
2. Either fingerprint or iris, mandatory biometric feature
3. Storage of the biometric feature in the shape of a digital image, mandatory
4. Storage of the biometric feature on a contactless chip on the travel document
5. Storage of the biometric feature in a central database
6. Biometric features to be used for the purpose of authentication and identification

European Community

The EC accepts the recommendations and standards established by ICAO. Within this framework, the EC prescribes
1. Face as a primary, mandatory biometric feature
2. Fingerprint as a secondary, optional biometric feature
3. Storage of the biometric feature in the shape of a digital image, mandatory
4. Storage of the biometric feature on a contactless chip on the travel document

DUTCH PROPOSAL

The Netherlands accepts the recommendations and standards established by ICAO, US and EC.
Within this framework, The Netherlands prescribe[2]
- Face as a mandatory biometric feature
- Fingerprint as a mandatory biometric feature
- Storage of the biometric feature in the shape of a digital image, mandatory
- Storage of the biometric feature on a contactless chip on the travel document

Iris technology is not included in the Dutch plans. The Netherlands chose to use biometrics for verification purposes, not only in border crossing but also in the social and fiscal domain.

It is the intention of the Dutch government to use biometrics only under surveillance.

SCOPE OF THIS THESIS

The plans of the EC for the implementation of biometrics in national identity management are in scope of this thesis. The plans of the US are in scope, only as far as they are constitutive for the EU plans.

The application of biometrics in national identity management is a many-facetted and complex operation.

Facets of the implementation are:
1. Technology of biometrics
2. Management of the (biometric) national identity infrastructure
3. Procedures connected to the application of biometrics
4. Public support
5. Dutch legislation
6. International context

Technology, infrastructure and international context are in scope of this thesis. Management of the (biometric) infrastructure and procedures connected to the application of biometrics are out of scope, as these are both not yet established.

The applicable European and Dutch legislation offers a background for the evaluation of the application of biometrics in national identity management and is contained in Appendices 6 and 7.

[2] Recent decision in the EC Commission ' JBZ-Raad'

CHAPTER 3 – RESEARCH

QUESTION

As the biometric technology is integrated in the broader national identity infrastructure, the added value of the application of biometric technology and the risks and threats attached to it are to be evaluated in this context.

In this thesis, I shall answer, within the framework of the EU plans for the application of biometrics in national identity management, the following questions:

Tactical questions
1. Describe current issues
2. Appraise the biometric features as proposed by US and European Community

Strategic questions
1. Analyse the implications of the application of biometrics in national identity management on a logical level
2. Analyse the risks attached to the application of biometrics in national identity management in daily practice, limited to the following issues:
   - Look alike fraud[3]
   - Multiple identities[4]
   - Identity theft[5]
3. Describe recommendations

Based on the analysis, as described above, I will conclude that the application of biometrics in national identity management as proposed by the EU is not feasible to fight identity fraud. This leads to a fourth and last research question:

4. Describe an alternative to the European Community proposal

APPROACH

Part II describes theory, facts and figures of national identity management and biometrics and consists of chapters 4, 5 and 6. This part is based on the study of literature and other sources about identity management and biometrics.

I do not find, in the literature on identity fraud, a solid theoretical framework for national identity management. Besides, the focus is mainly on identity document fraud, not on the spectrum of methods of identity fraud as a whole. Therefore, in chapter 4, I will start to construct a theoretical framework.

In chapter 5 and 6, I will describe the facts and figures of national identity management and biometrics technology in general.

[3] In case of look alike fraud, frauds use identity documents which belong a look alike
[4] Frauds use multiple identities in order to take (multiple) advantage of public and private services or to hide criminal traces. Multiple identities may occur as:

Shared identities	a subject has more than one identity document containing the same (his or her own) personal data and the same (his or her own) biometric feature
Homonym identities	a subject has more than one identity document contaning the same (his or her own) personal data and more than 1 biometric feature
Synonym identities	a subject has more than one identity document containing different personal data and just one (his or her own) biometric feature

[5] In case of identity theft, a fraud manages to claim the identity of another subject, by getting registrated under the other person's name and using an identity document containg the other subjects personal data

In Part III, I present a tactical approach of biometrics in national identity management. This part consists of chapters 7 and 8.

Much has been said about the quality of biometric technology as such. Many publications deal with national identification systems, identity, identity fraud and identity documents. Only a few publications deal with tactical issues concerning national identity management and the role of biometric technology.

In chapter 7, I will discuss tactical issues concerning the application of biometric technology in national identity management.

In chapter 8, I will appraise the biometric features as proposed by US and European Community.

Part IV contains an appraisal of the proposed application of biometrics on a strategic level and consists of chapters 9, 10 and 11.

Chapter 9 describes the implications of the application of biometrics in national identity management on a logical level.

In chapter 10, I describe the risks attached to the application of biometrics in national identity management on the basis of a scenario analysis.

Chapter 11 consists of a number of strategic recommendations.

Each of the chapters will be followed by a partial conclusion.

In Part V, I will present an integrated conclusion.

II – THEORY, FACTS AND FIGURES

CHAPTER 4 – THEORY OF BIOMETRICS AND NATIONAL IDENTITY MANAGEMENT

BIOMETRICS

Biometrics – basic concepts

Table 1 – Biometrics - basic concepts[6]

Biometrics	The science of measuring individual physical features (hereafter: biometric features)
Biometric identification	Individual biometric features are established and compared to biometric features of individuals in a database, the identity of the individual can be established if the individual's biometric feature match with one of the biometric features stored in a database or chip
Biometric authentication	Individual live biometric features are established and compared to biometric reference data of the same individual stored on an identity document (on a chip); the authenticity of the identity claim is established if the individual's biometric feature matches the biometric feature stored on the identity document; Thus, *biometric authentication* is synonymous with *biometric verification*

The application of biometrics, in the context of *national identity management,* aims at authentication, i.e. the authenticity of the identity claim is established by comparing biometric features stored on the identity document with live biometric features.

[6] The definitions in this table are my own, in my opinion the sources I studied did not offer a set of satisfying and consistent definitions.

General criteria for biometric features

Not every physical feature is feasible for biometric application. In order to be successful, biometric features need to match as a minimum, the following criteria:

Table 2 – General criteria for biometric features[7]

Uniqueness	an identical trait won't appear in two people
Universality	occur in as many people as possible
Permanence	don't change over time
Measurability	are measurable with simple technical instruments
User friendliness	are easy and comfortable to measure
Fraud resistance	are difficult to copy and spoof

Types of biometric features

The following factors contribute to the constitution of a physical feature [45]:

Table 3 – Types of biometric features

Genotypic features	Show hereditary determined variations, established in the DNA: unchangeable
Randotypic features[8]	Show random variations in the biometric feature are created during the early phases of an embryo's development: (often called phenotypic): unchangeable
Behavioural features	Variations in movement and expression, due to learning and training, are subject to change

This is a general distinction made in literature. As a rule, both genotypic, randotypic and behavioural factors contribute to the development of a biometric feature, although to varying degrees. Pure behavioural features in general are highly impermanent and not unique and are therefore not feasible for biometric applications.

Table 4 – Public versus private biometric features

Public biometric features	Public biometric features (from living subjects) are easy to access and to copy or imitate, examples: iris, face, voice and finger
Private biometric features	Private biometric features (from living subjects) are not easily accessed and very difficult to copy or imitate, example: hypodermic vein patterns

The distinction between public and private features is not made in the literature. The distinction however is highly relevant, for it affects directly the ability of subjects to keep their biometric features safe and secret.

If subjects cannot protect their biometric features against unauthorised access, they are easy victims for frauds who want to abuse their biometric features or even steal their identity. Of course, liveness detection might prevent successful spoofing of biometrics. However, liveness detection is not always successful. Furthermore, as I pointed out before, biometrics are common across functions. A copy of a biometric feature, within a particular document chain, might be used for spoofing in another document chain.

[7] The criteria mentioned are frequently mentioned in the sources I studied. I choose to use the definitions of these criteria as given in [45], in my opinion, they are to the point and need not to be improved or re-invented.

[8] I prefer the term randotypic over the term phenotypic. The linguistic root of the term 'randotypic' is random, thus, by using this term I refer to the concept of randomness, which is exactly what we are looking for when we build identification infrastructures. The term 'phenotypic' stresses the fact that the features is influenced by particular circumstances. For example, body length depends, among other things, on the quantity and quality of food available. Body length is not a random physical feature and therefore not a suitable feature for biometric technology.

IDENTITY

Elements of identity

Table 5 – Elements of identity

Biometric identity	Description of physical features of an individual, including DNA, face, fingerprint; synonym with 'physical identity'
Attributed identity	Description of data attributed to an individual, including full name, date and place of birth, parents name
Biographical identity	Biographic descriptions, may include education, electoral register entries, criminal record, benefits claimed and taxes paid, employment, mortgage and property, insurance, interactions with banks, creditors, utilities, public authorities

Identity versus national identity

Table 6 – Identity versus national identity

Identity	A persons *identity* is a set of characteristics – biometric, attributed and biographical – that fully describe and characterises that person as an active member[9] of human society and differentiate him or her from the rest of the population The *appreciation* of the identity of a person depends on the context or society in which the identity is established. In one context, for example mathematics, the identity of subject may be described as 'brilliant' whereas in another context, for example sports, the identity of the very same subject may be described as 'inferior'. Authorisations assigned to a particular identity are based on the appreciation of a that identity.
National identity[10]	A persons *national identity* is a set of characteristics – biometric, attributed and biographical – as established and registered in the National Population Register

[9] A person becomes an active member of society once he or she is recognized as such by society. An unborn baby, for example, is usually not recognized as an active member of society. Neither are slaves nor prisoners in extermination camps.

[10] I am aware that the term *national identity* is a homonym. The term as I define it here, in the context of *national identity management*, is not te be confused with the term *national identity* as defined in the context of *nationalism, national proud or folklore*. Nonetheless, I do not know a term which describes better what I am talking about. Any suggestions are welcome.

IDENTIFICATION, AUTHENTICATION AND VERIFICATION

Identity document, identification, authentication and verification are in the context of this thesis defined as follows:

Table 7 – Definitions of identification, authentication and verification

Identification is in the context of this thesis to be understood as the determination of national identity. In other words, identification is the action or process of determining who a person is in the national context, using the identity records created- and identity documents issued by the government. An *identity document* serves as a legal instrument for *identification* in the context of national access control (border crossing, public and private services) and in the social and fiscal domain. It establishes the national identity of an individual by describing one or more aspects of biometric, attributed and biographic identity. *Authentication* is to be understood as: - The determination whether the *identity* as claimed by an individual is his or her true identity, i.e. whether the claimed identity matches with the individual who claims it; and - The determination whether the *identity document* as shown by an individual is a true identity document, i.e. whether the identity document is truly issued by the government and the information on the document is not forged. *Verification* is a special instance of authentication, Verification is to be understood as the determination whether the *identity claim,* based on an *identity document*, is true. In other words: whether the identity described by the document shown matches with the identity of the individual showing the document. *Currently, data about the document holder, like a photograph, date of birth and length serve as an instrument in the verification process.* *Biometric verification* is to be understood as verification based on biometric features. For this purpose a biometric feature stored on the document is compared with the live biometric feature of the individual showing the document. *In the future, biometric data will serve as an instrument in the verification process.*

NATIONAL IDENTITY MANAGEMENT

Basic concepts

Basic concepts like identity fraud, document fraud and travel document fraud, are frequently used as equivalents, which is very confusing. The basic concepts used in risk analysis have to be clearly defined. In defining these concepts, I take the terminology of Dr. Mr. J.H.A.M. Grijpink as a starting point. In 'Identiteit als kernvraagstuk in een informatiesamenleving: een pleidooi voor een ketenbenadering' [30], Grijpink pleads for *a value chain perspective*. He points out that identity is to be viewed as the product of a value chain in which hundreds of organisations work together in order to prevent identity fraud.

The *national identity chain* is to be understood as a number of consecutive acts and products. These enable the establishment and verification of *national identities* and *national identity documents* in a country. Thus, *identity* is a product of an *identity chain* and has many manifestations, for example *source document*, *travel document* and *visa*. The *ultimate identity chain*, in my opinion, is a worldwide phenomenon, extending from the swamps of Bangladesh and the caves of Afghanistan to US- and European government offices. One tiny error early in the chain renders the rest of the chain invaluable.

Grijpink concludes that *the national (Dutch) identity* chain is deficient in many respects. Major improvements are necessary.

On the basis of the concept of value chain, I define the following concepts.

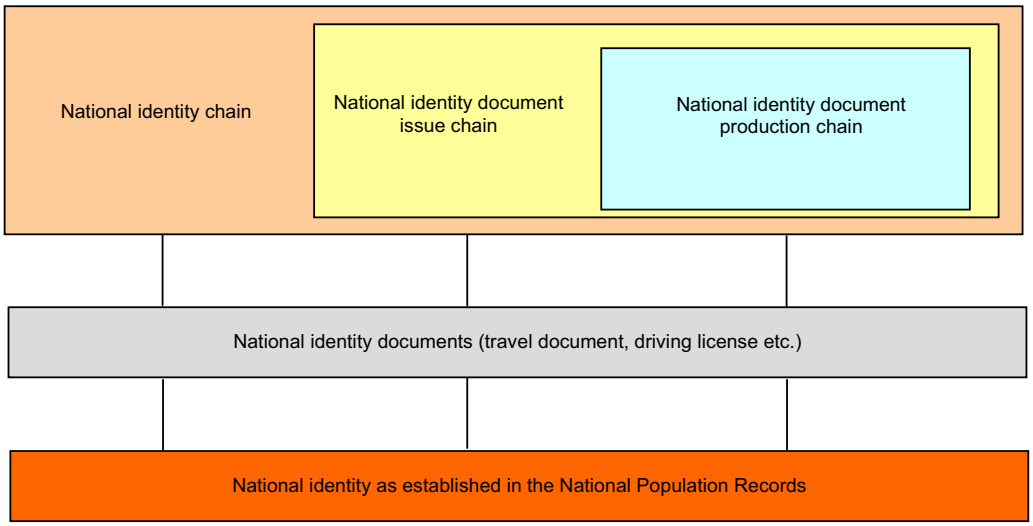
Table 8 – Basic concepts in national identity management

National identity document *production* chain	The organisations who co-operate in the production of identity documents
National identity document *issue* chain	The organisations who co-operate in the issuing of national identity documents
National identity chain	The organisations who co-operate to establish and verify identities in the context of national identity management
Source documents	Third party statement, issued by either a public or a private party, on the identity of a subject, serves as a prerequisite to obtain an national identity document, within the same country or abroad
National identity document *chain* fraud	Type of fraud by which the national identity document *chain* is manipulated with the intention either to obtain a national identity document on the basis of false presumptions or false information; or by claiming an identity on the basis of false presumptions, for example false or forged non-national identity documents or source documents or forged national population records
* Document *chain* fraud[11]	Type of fraud by which a specific identity document *chain* is manipulated with the intention either to obtain an identity document on the basis of false presumptions or false information; or by claiming an identity on the basis of false presumptions, for example false or forged non-national identity documents or source documents Example: *travel document chain* fraud
National identity *document* fraud	Type of fraud by which a false or forged national identity *document* is used either to claim a false identity or to obtain a new false identity document
* *Document* fraud	Type of fraud by which a specific false or forged national identity *document* is used either or to claim a false identity or to obtain a new * *document* Example: *travel document* fraud

[11] The asterisk is to be read as a wild card symbol, i.e. * document chain fraud includes *travel* document chain fraud as well as *driving licence* chain document fraud; * document fraud includes *travel* document fraud as well as *driving licence* document fraud

Schematic overview

Figure 1 – Schematic overview of national identity management



Contrary to Grijpink, I do not include source documents in the definition of national identity chain. Source documents are part of an external domain and are often of foreign origin. They are not a link in the chain but rather a precondition for the establishment of the chain. However, as such, source documents have an impact on the quality of the chain. See below for a further comment on source documents.

Explanation of the scheme (Figure 1)

In the above scheme, the correlation between the respective chains is made clear.

The *production of identity documents forms a chain in itself* and is a part of the document issuing chain. The production of identity documents consists of a chain of suppliers and a production infrastructure.

The *national identity document issuing chain* consists of a chain of municipal offices. The municipal offices are responsible for the national population records. The national identity document issuing chain is a part of the national identity chain.

The *national identity chain* consists of a number of identity administrations, which are linked to a particular purpose or domain (travelling, driving). The authorities, responsible for these identity administrations, depend for the integrity of the personal data on the national population records of the registered subjects and thus on the municipal offices which are responsible for these records.

Thus, the concept of *identity chain* is an abstraction. As there are more types of *identity documents*, there are more types of *identity chains*, for example the *travel document chain*, the *identity card chain* etc.

The concept of *identity* is an abstraction as well. There are more types of *identity chains*; consequently, there are more types of *identities*, for example *travel (document) identity* and *driving (license) identity*. All these identities are linked, because they are fully or partially or based on the *national identity* of a subject, which is established in the national population records.

The identities established in the respective domains are based on the national identities as established in the National Population Registers and thus linked. In other words, because the

national identity document chains are part of the *national identity chain*, they are mutually dependent.

The quality of a particular type of identity document has an impact on the effectiveness on the national identity management as a whole.

Identity documents are *instruments for identification in the context of access control*, whereas source documents are *prerequisites to establish a national identity and to obtain a national identity document*. Thus, travel documents, foreigner documents, driver licenses are all included in the definition of national identity documents as well as visa. Because source documents are just a prerequisite to obtain a national identity I exclude them from the definition of national identity documents.

National identity management and biometrics

Table 9 – Biometrics in national identity management

National identity management deals with strategic, tactic and operational aspects of creating and maintaining identities and identity records by the government The application of biometric technology on *national identity documents* is to be considered as a contribution to and integrated part *of national identity management*

Again, we have the look at the scheme of national identity management (Figure 1).

Biometric features are, once used, by definition, common through all identity chains. Vulnerabilities in the application of biometrics within a particular identity chain have an impact on the reliability of other identity administrations within the national identity chain.

CHAPTER 5 – FACTS AND FIGURES ON NATIONAL IDENTITY MANAGEMENT

THE QUALITY OF NATIONAL IDENTITY MANAGEMENT

The quality of population records is unsatisfactory and insufficiently monitored. Research of Arre Zuurmond [46] demonstrates that information the quality of the population records differs substantially between different registrations and the registered data often do not match with reality. Between 5% and 90% of the data is said to be incorrect. For this reason, the Dutch police do not trust the official population records and has set up a population administration of its own [55].

In the Dutch context, responsible parties do not take detection and prevention of identity fraud seriously. Authorities suffer from a lack of vision, strategy and insight in the complex issues of identity management. A lack of co-operation in detection and prevention of identity fraud further worsens the situation [3].

FRAUD IN NATIONAL IDENTITY MANAGEMENT

The phenomenon of fraud is a blind spot by definition

The literature about identity fraud does mention but not solve a problem inherent to the detection and prevention of fraud. We all know fraud exists but we do not know to which extent or which types of fraud are most popular. We only know about the fraud we are detecting.

The extent of detected fraud is only the top of the iceberg. Fraud is a blind spot by definition, which we cannot eliminate; nevertheless, we should be aware of it.

In an article called 'Grootschalige biometrie is jongleren' [7], a representative of the Dutch Ministry of Social Affairs and Employment states that *look alike fraud* is not an issue. He concludes that this type of fraud seldom occurs. A representative of the Immigration and Naturalisation Services says that no data are available on look alike fraud, in her opinion this means that look alike fraud is therefore not an issue.

Probably for this reason, authorities often tend to take a post factum approach to identity fraud.

Fraud, look alike fraud in particular, is on the agenda

Hein Blocks, the director of the Nederlandse Vereniging van Banken (Dutch Bank Association) approves that look alike fraud has been detected 234 times in 2000. The Royal Military Police too, is well aware of many types of fraud, look alike fraud included [3].

The Dutch Ministry of the Interior and Kingdom Affairs takes look alike fraud serious as well. However, this might be due to major problems with travel documents in the past. The stable door was locked after the horse has bolted. This may help, but is not a guarantee for deliberate decisions in the future.

Identity fraud is perceived by the government as an external risk

It strikes me that, generally spoken, look alike fraud is taken more seriously by the private sector then by the public sector. This is probably due to the fact, that for the public sector, the consequences of fraud are *external* whereas the private sector has to bear the consequences itself. In general, the risks attached to national identity management are mainly *external* to the government and *internal* to the citizens. Because of this, responsible parties i.e. governments are not stimulated to mitigate risks effectively. However, the main task of the government is to serve the interest of the citizens. Thus, mitigation of these external risks is by definition core business for governments.

The true stakeholders i.e. the citizens may try to prevent loosing their own documents, but apart from that, they have a limited ability to mitigate these risks.

The perception of risks of identity fraud as being mainly external is a risk in itself. This applies to governments in particular.

Identity fraud is extensive and increases rapidly

The extent of identity fraud is large and the increase in identity fraud over the last five years is alarming. A number of factors contribute to the large extent and growth of identity fraud. The number of identity checks increases rapidly and, due to this, the 'need' for identity fraud grows.

The financial cost of identity fraud to society is enormous and so are probably the immaterial consequences. Based on recent figures (2000-2001) [20], I estimate that identity fraud costs 5.5 billion Euro yearly as a minimum: 150.000 identity documents (travel documents only) are either stolen or missing; a missing document costs 36.300 Euro. Immaterial damage, risks and indirect costs are not included. Neither are included the costs connected to secondary types of fraud and crime, based on identity fraud, such as illegal immigration, human trafficking, international crime and terrorism, money laundering and identity theft.

In other words, there is a strong business case to fight identity theft. Considering the estimated costs to society, it is justifiable to spend at least a budget of 55 million Euro, to achieve an improvement of only 1%.

CONCLUSIONS CHAPTER 5

<Sub conclusion 5.1> Fraud is a blind spot by definition. The approach of fighting identity fraud should therefore be ante factum and based on scenario analysis rather than on statistics.

<Sub conclusion 5.2> Both government and citizens tend to perceive the risks of identity fraud as external. Consequently, the risk of identity fraud is not properly mitigated.

<Sub conclusion 5.3> Identity fraud is extensive and growing fast. There is a strong business case for the improvement of national identity management and for fighting identity fraud. Considering the costs of identity fraud to society, the budget to improve the situation is available. Governments in some cases lack a coherent vision and strategy in order to improve national identity management.

<Sub conclusion 5.4> The quality of national identity management is insufficient. If we don't improve the quality of national identity management, other improvements, like the application of biometrics, are ineffective. The application of biometrics might create an unfounded trust in the effectiveness of in national identity management, which is a risk in itself.

CHAPTER 6 – BIOMETRICS: FACTS AND FIGURES

PERFORMANCE OF BIOMETRIC TECHNOLOGY

Performance indicators and criteria for success

In the literature on biometric technology a number of performance indicators are mentioned. Though not the inventor, Rudolf L. van Renesse offers a good overview of performance indicators of biometric technology in “Implications of biometrics on travel-documents” [6].

The performance is measured in terms of False Acceptance Rate (FAR)[12] and False Rejection Rates (FRR)[13]. Systems can be configured to produce a lower FAR at the cost of a higher FRR and vice versa. It is evident that a low FAR is desirable. However, a high FRR is inconvenient and may cause many people to resort to fallback procedures; people might even pretend to be falsely rejected for this reason, claiming that the performance of the system is miserable.

The operating point of the system determines the relative proportion between FRR and FAR. Fallback procedures should be robust in order to deal with the type of frauds who want to resort to fallback procedure.

Implementing multiple verification attempts in the verification process causes a decrease of FRR while the FAR remains constant; exact numbers depend on the specific technology applied.

However, the performance of biometric technology is notoriously sensitive to sensor/capture quality [10]. The reason is that a bad sensor partly destroys or diminishes the information of both live and stored biometric feature, but in different ways. The quality of the compared features is lower, and so is the quality of the evaluation.

There is a significant difference between the evaluation of biometric technology by independent laboratories and by suppliers. According to suppliers, biometric technologies score approximately 10% better than the performance indicated in the independent laboratory’s evaluations. This is probably not much of a surprise, but it stresses the necessity for an independent evaluation of technology before actually applying it.

The best fingerprint technology uses algorithms based on pattern recognition. This is probably not a coincidence. There is also a possibly a correlation between the performance and fraud resistance and the applied different algorithms. It might therefore be useful to evaluate the performance of biometric algorithms rather than biometric technology as such. This is a subject for further research.

Factors influencing the performance of biometric technology

The influence of age, race, psychology and gender

Age, race, psychology and gender have a major influence on the performance of biometric technology but exact information is not yet available.

Ageing, for example, might cause the validity of the biometric image to decrease by approximately 5% per year [57]. If this appears to be true, this is a serious, probably insurmountable, shortcoming of biometric technology, considering that the minimal life cycle of identity documents is five years!

[12] The False Acceptance Rate (FAR) indicates the number of times (as a percentage of the total number of verifications) that a subject is falsely accepted when comparing the biometric feature against a stored biometric feature.
[13] The False Rejection Rate (FRR) indicates the number of times (as a percentage of the total number of verifications) that a subject is falsely rejected when comparing the biometric feature against a stored biometric feature.

Cees Bosveld of the Dutch Military Police and expert in the field of forensic identification states that he never ran into a fingerprint changing due to ageing. In his opinion, the size of the fingerprints may change, but certainly not the pattern.

This might be due to the following reasons:
- Fingerprint recognition systems do not adapt well to changes in size (laboratory research is necessary to find out); or
- Most matches as a result of searching forensic database concern relatively recently created records casu quo recently recorded biometric features; statistical analysis can reveal if this is the case); or
- Both (1) and (2).

Asker Bazen [56] developed an algorithm that compensates for elastic distortions. This algorithm is not operational. It would be interesting to find out, whether this algorithm has a positive impact on the problem of ageing.

In the appendix to the report 'Biometrics in Travel documents', called 'Suitability of face recognition for look-alike detection' [16], Dr. L. Moro Ellenberger and Drs. E.D. Schoen describe that systems perform different for different ethnic groups. Face recognition systems in particular need to be trained for ethnic groups. However, when comparing the results of different systems together, no preference is noticed.

In addition, the authors [16] indicate that some systems create lower similarity numbers for women.

Thus, technical systems seem to be similar to human beings: systems reflect unconscious and unintentional intentions, pre-occupations and limitations of the people who designed, developed and tested them. Sexism, racism and ageism of biometric systems cannot be excluded [49].

The influence of the conditions of enrolment and verification

Enrolment and verification need to be acquired under *exact* the same conditions. Moreover, scanned photograph result in lower similarity numbers, a low threshold has to be chosen in order to recognise somebody as him- or herself [16]. From this, the conclusion is drawn, that empirical comparison of face recognition by human trained officers and face recognition software is necessary to determine the usefulness of face recognition technology.

The influence of environmental factors

Environmental factors cannot always be controlled, as in the case of people entering a checkpoint when it is cold or rainy outside, or warm and damp inside.

The influence of social psychology and society

Psychological factors, which are of influence, are:
1. Social environment and public security;
2. Legal context: the sanctions of the sharia on theft for example differ from the sanctions defined by the law in democratic societies;
3. The context of the society: for example threats of war, violence or terrorism;
4. Motivation and perception of citizens: for example fear of identity theft or big brother;
5. Acquaintance with biometric technology;
6. Culture: for example taboos on physical contact or showing the face; and
7. Literacy

Psychological factors are hard to control. Each of the environmental and psychological factors might probably have a negative influence of 5% on the performance of biometric technology. What might be the consequence if we combine two, three or more of these factors? Or else, what is the best-case scenario, and what is the worst-case scenario?

According to an expert in this field, Jim Wayman [49], we don't know yet. We don't know how to combine the errors caused by these factors because we lack data on error correlation. In other words, what is 5% + 5% + 5%?[14] It is something between 5% and 15%, but we can't be more certain about the value than this because the correlation are unknown".

The importance of liveness detection

Spoofing of life biometric features is an attractive and easy alternative to being genetically related. In case of iris recognition, lenses may be used, in case of finger recognition, thin rubber or silicon film; and in case of face recognition, plastic surgery and heavy make up. Spoofing is an attack in the analogous domain, relatively easy to perform and therefore attractive for frauds.

The spoofing of biometric features exposes well behaving citizens to the risk of theft of their biometric features, or even their identity. This stresses the importance of high quality, liveness detection mechanisms.

Without high quality liveness detection, the application of biometrics is not resistant to fraud.

Performance in large-scale applications

Current data on performance are based on laboratory- or small-scale applications.

Van Renesse [6] states that the FRR of different systems, in 'the harsh practice of heterogeneous user groups' do not show significant differences between them and are approximately found in the range between 1% and 5% (given a fixed FAR). If his is true, the performance biometric technology depends to a relatively high degree on external factors and not on inherent quality. However, I find the difference between 1% and 5% significant. The meaning of 'harsh' and 'heterogeneous' in this context however is not clear to me. Neither is clear whether the samples of people are statistically representative in respect of race, age, gender and psychology.

We have no strong indication about the performance of worldwide applications of biometrics in heterogeneous user groups. We therefore cannot predict the performance of biometrics in national identity management, as currently proposed by US- and EC governments.

Performance in groups of look alikes

In case of look alike fraud, sisters or brothers often 'lend' identity documents to each other. Their biometric features are genetically related and more often than average mutually dependent. This has a negative impact on the overall performance of biometric technology and limits the positive impact of combined biometrics. With face recognition- and fingerprint technology in particular, we see a decrease in performance with family relations.

Suppliers indicate that the problem of biometric look alike fraud has not yet been tackled.

Frauds are often literally 'sisters and brothers in look alike fraud'. Because of this, tests on a sample of genetically closely related subjects are necessary, in order to make sure the proposed technology is feasible to solve the problem of look alike fraud.

Look alike frauds do not look alike. Dr. L. Moro Ellenberger and Drs. E.D. Schoen [16] found that look alikes detected by biometric systems do not show any similarity in appearance according to the human eye. If the attention of authorities in charge shifts from looking at a face (analogue domain) to looking for a green light at a biometric device, the increase of risk is significant.

[14] The percentages mentioned here are estimated by Jim Wayman. But, for the sake of a thought experiment, the exact value does not matter. The thought experiment shows us the grade of uncertainty we are dealing with: we know neither the exact percentages, nor do we know the rules how to add up.

SECURE DEVELOPMENT AND IMPLEMENTATION

Evaluations of biometric infrastructures show that the implementation demands attention. In one case, serious inaccuracies were found in the implementation of the biometric infrastructure. Keys in plaintext were transported repeatedly over the line between the verification peripheral and the processing unit, along with the encrypted information. In addition, source code was stored on 'production' processing units[15].

Secure development and implementation of the biometric infrastructure is an important issue that, if not taken seriously, can put the reliability of the application of biometrics as a whole at risk.

CONCLUSIONS CHAPTER 6

<Sub conclusion 6.1> There is no strong indication about the performance of worldwide application of biometrics in large heterogeneous user groups.

<Sub conclusion 6.2> In order to evaluate the effectiveness of biometric technology as an instrument against look alike fraud, it needs to be tested against a group of genetically related subjects.

<Sub conclusion 6.3> Insufficient data are available on the fraud resistance of biometric technology.

<Sub conclusion 6.4> A shift of attention of the authorities in charge of verification from the analogue domain to the digital domain poses a secondary risk. Subjects who are look alikes according to the system, aren't look alikes in real life and vice versa.

<Sub conclusion 6.5> Spoofing of biometric features exposes well behaving citizens to the risk of theft of their biometric features, or even identity theft. High quality liveness detection is necessary, to protect innocent citizens against these negative side effects.

<Sub conclusion 6.6> Secure development and implementation of the biometric infrastructure is an important issue that, if not taken seriously, can put the reliability of the application of biometrics as a whole at risk.

[15] For security reasons, I do not reveal on which implementation this information applies.

III - TACTICAL CONSIDERATIONS

CHAPTER 7 – BIOMETRICS IN NATIONAL IDENTITY MANAGEMENT

CURRENT ISSUES IN THE APPLICATION OF BIOMETRICS

Mandatory versus voluntary application of biometrics

The distinction between mandatory and voluntary application of biometric technology is relevant. Mandatory application may cause many zero effort attacks. Malicious document holders may claim false rejects, sabotage the enrolment procedure or the biometric functionality of the document chip or mutilate relevant biometric features, in order to use relatively weak fallback procedures.

According to Van Renesse [6], this constitutes a major risk, which can be (partially) mitigated by using a central database in which biometric features are stored. However, the risks shift from one place to another: databases can be hacked and social and political resistance can lead to a rejection of biometric technology as such.

Voluntary application is not hampered by zero effort attacks; this leaves more time and resources for strong fallback procedures. However, fallback procedures will always be relatively weak, because they allow attacks in the analogous domain whereas attacks in the digital domain are relatively hard to make.

Domestic versus international application of biometrics

A conference paper by Rudolf van Renesse, 'Implications of biometrics on travel-documents' [6] is interesting in this context. Van Renesse observes, that the improper use of biometric verification abroad may lead to unfounded accusations. Thus, travel document holders are exposed to the risk of being falsely accused of look alike fraud, of theft of their biometric features or even identity theft.

It is relatively easy to impose rules for the secure implementation and privacy protection within national borders but it is much more difficult to impose these rules abroad, let alone to check whether these rules are followed. Malicious parties, in either public or private domain, might illegitimately use biometric devices to collect biometric features from innocent citizens and abuse these when pursuing criminal goals.

EXAMPLES OF THE APPLICATION OF BIOMETRICS IN NATIONAL IDENTITY MANAGEMENT

Until now, only Malaysia applied biometric features to passports. Some parties mention Malayan application as an example of a large-scale application to be compared to the EU plans. As such, much is to be learnt from the Malayan example.

Concerning purely technical issues, this might be true. However, as I pointed out before, success or failure of applications of biometric technology strongly depends on non-technical factors as well. Malaysia is an Islamic country and the sharia is applicable to its citizens. Who would dare to travel to or from Malaysia or claim services, using a stolen or forged document and take the risk of your hand being cut off? Much can be learnt for sure, but only with a critical approach.

Examples of the application of biometrics in national identity management are not available in the Western era. Consequently, no data on the added value of biometrics in national identity management are available.

CONCLUSIONS CHAPTER 7

<Sub conclusion 7.1> Voluntary application of biometrics in national identity management is advisable. Mandatory application may cause zero effort attacks. Voluntary application is not hampered by zero effort attacks. Voluntary application of biometrics in national identity management leaves more time and resources for high quality fallback procedures.

<Sub conclusion 7.2> Use abroad of biometric national identity documents exposes citizens to a higher risk of being falsely accused of look alike fraud, of theft of their biometric features or even identity theft.

< Sub conclusion 7.3> No relevant data on the performance and effectiveness of biometrics against fraud in national identity management are yet available.

CHAPTER 8 – BIOMETRIC FEATURES AS PROPOSED BY US AND EU

In order to judge the performance of particular biometric for the application in national identity management, specific criteria are needed. The technology has to be both reliable and efficient, even for large and heterogeneous groups and for those who are unwilling to co-operate. Circumstances for verification will often be demanding and difficult to control.

PERFORMANCE CRITERIA FOR SUPERVISED PASSAGE

The intention of the Dutch government is to apply biometrics only under supervision. Rudolf van Renesse [6] specifies the following criteria for supervised passage:

Table 10 – Performance indicators for supervised passage[16]

FAR	0,1%
FRR	5%
FTE[17]	p.m.

In the literature on biometric in national identity management I did not find a justification for these criteria. Until now, these criteria have not been subject of a systematic discussion.

The specified criteria are arbitrary. With the application of biometrics, the government intends to fight looks alike fraud. Considering the fact that the performance of biometric technology is considerably worse for look alikes (see below), these criteria need to be reconsidered.

PERFORMANCE OF BIOMETRIC TECHNOLOGIES

Laboratory performance of biometrics against criteria for supervised passage

As said before, these performance criteria are based on assumptions and it is not sure whether these are realistic. They could be either too pessimistic or too optimistic.

Below some figures of independent laboratory tests and of suppliers on the performance of biometric technology.

Table 11 – Independent laboratory's and suppliers' performance data

	Independent laboratory tests				Suppliers tests			
	Minimal %		Maximal %		Minimal %		Maximal %	
	FAR	FRR	FAR	FRR	FAR	FRR	FAR	FRR
Face	1	**3**	**10**	**9**	0,1-1	**0,1-1**	**1,5**	**1,5**
Iris	**<0,1**	**2**	--[18]	--[19]	**<0,01**	**0,5**	**0,01**	**0,1**
Finger	**0,1**	**8**	**0,1**	**10**	**0,01**	**0,01**	**0,1**	**2**

This also includes an evaluation against the performance criteria, as follows:

BLUE FAR / FRR matching criteria
BLUE FAR / FRR nearly matching criteria
RED FAR / FRR not matching criteria

We may conclude that iris technology is the best match against the specified criteria, followed by finger technology that has an acceptable FAR but only in combination with an unacceptable FRR. Face technology does not match the criteria.

The objection often made against the application of iris technology is that there is only one supplier on the market and the algorithm applied is proprietary and secret.

[16] Derived from "Implications of biometrics on travel-documents", Rudolf L. van Renesse [6]
[17] FTE stands for: failure to enrol, the inability of a subject to show a feasible biometric feature; in case of missing fingers or eyes or a mutilated face. Also, skin deseases can cause a failure to enrol a fingerprint.
[18] Values not determined (not enough data available)
[19] Values not determined (not enough data available)

This is not correct. Currently, already six vendors are offering iris technology [50]. It is worthwhile to find out whether the applied algorithms are secret, and, if not, to evaluate these algorithms. This is, in the context of this thesis, out of scope and a subject for further research.

Impact of sex, race, age and psychology on the performance of biometrics

According to Jim Wayman [49], sex, race, age, and psychology are factors, which may probably have a negative influence on the performance of biometric technology of 5%. We don't know what the result might be if we combine these factors, because the mutual correlation is unknown. The negative influence is therefore something between 5 and 20%.

Table 12 – Influence of sex, race, age and psychology on performance

	Negative impact 5%				Negative impact 20%			
	Minimal		Maximal		Minimal		Maximal	
	FAR	FRR	FAR	FRR	FAR	FRR	FAR	FRR
Face	**1,05**	**3,15**	**10,5**	**9,45**	**1,2**	**3,6**	**12**	**10,8**
Iris	**<0,105**	**2,10**	--	--	<0,12	**2,4**	--	--
Finger	0,105	**8,4**	**0,105**	**10,5**	0,12	**9,6**	0,12	**12**

This also includes an evaluation against the performance criteria, as follows:

BLUE FAR / FRR matching criteria
BLUE FAR / FRR nearly matching criteria
RED FAR / FRR not matching criteria

If we take into consideration the impact of sex, race, age and psychology, we may conclude that iris technology is the only possible match against the specified set of criteria. However, due to a lack of data on maximal FAR and FRR, we cannot be sure.

Finger technology is an option only if we accept a relatively high FRR.

Performance of biometrics in a population of look alike frauds

The criteria above refer to the population as a whole. However, we need not to control well-behaving citizens. The subgroup of well-behaving citizens will never be falsely accepted. The target group of biometrics is by definition a group of frauds. The Dutch government intends to apply biometrics in order to detect ill-behaving citizens, trying to commit look alike fraud. The effectiveness of biometrics is therefore to be evaluated against the subset of look alike frauds. Part of these look alike frauds are genetically related, we don't know exactly how many.

Suppliers indicate that the problem of look alike fraud has not yet been tackled and it is an understatement to say that technology for liveness detection is not yet fully developed. In my opinion, this is most worrisome considering the fact that detecting look alike fraud is said to be the raison d'être of applying biometric technology in Dutch national identity management [8]. Further research on the performance of biometric technology in populations of genetically related subjects is necessary.

However, imagine that 50% of the look alike frauds is genetically related. It is very likely that relatively many of these look alikes are falsely accepted. But this is hard to predict. Below, I extrapolate a hypothetical negative impact of respectively 20% and 40% related to the performance figures as shown in the table above. I.e. in column 1, we find a relatively positive scenario: a negative impact of a look alike population of 20% calculated on top of a negative influence of 5% due to the influence of sex, race, age and psychology. . In column 2, we find a worst case scenario: a negative impact of a look alike population of 40% calculated on top of a negative influence of 20% due to the influence of sex, race, age and psychology.

Table 13 – Hypothetical evaluation in a population of look alike frauds

	Negative impact 20%				Negative impact 40%			
	Minimal		Maximal		Minimal		Maximal	
	FAR	FRR	FAR	FRR	FAR	FRR	FAR	FRR
Face	**1,26**	**3,78**	**12,6**	**11,34**	**1,68**	5,04	**16,8**	**15,12**
Iris	<0,126	**3,456**	--	--	<0,168	**3,36**	--	--
Finger	0,126	**10,08**	0,126	**12,6**	0,168	**13,44**	0,168	**16,8**

This table includes the evaluation against the performance indicators for a population of look alike frauds, as follows:

BLUE FAR / FRR matching criteria
BLUE FAR / FRR nearly matching criteria
RED FAR / FRR not matching criteria

We may conclude that iris technology is the best match against the specified criteria and thus is the only effective instrument against look alike fraud.

It is not sure whether iris technology completely matches the performance criteria for a group of look alike frauds. Further research on the performance of iris technology, within groups of genetically related subjects is necessary.

An extra argument in this respect is the fact that the iris is a randotypic biometric feature. Consequently, it will perform best within a group of subjects who are strongly genetically related. Due to this, the performance within a group of look alikes will probably fully match the specified criteria. Finger patterns and faces are both relatively strong genotypic biometric features and will vary less within a group of subjects who are strongly genetically related.

Further research on the performance of biometric technology, iris technology in particular, within groups of genetically related subjects, is necessary.

Effectiveness of biometrics in national identity management

The performance of biometric technology is only one of a number of factors, which have an impact on the effectiveness of biometric technology in national identity management.

It is difficult to measure the impact of these factors in laboratory environments. The overall effects of these factors in large-scale applications are therefore to be estimated.

Table 14 – Factors of impact on the effectiveness of biometrics

CATEGORY and Factor	Explanation	Comment
ABILITY TO ENROL		
Universality	Occur in as many people as possible; ethnic groups should not be excluded as a whole	Fingers and eyes can be mutilated or lost; faces are in general relatively intact; Within in the Asian population for example, fingerprints are weak and thus fingerprint technology is relatively without effect in this respect.
Successful enrolment	Ability to enrol feature	Face and finger can be temporary mutilated or modified, the modification of the iris is more difficult, painful and irreversible
ACTUAL PERFORMANCE		
Performance indicators	Performance of biometric technology (as established in the table above, including negative influences of race, age, sex and psychology)	Uniqueness is included in this factor, a lack of uniqueness resulting in a higher FAR
Environment independence	The independence of performance on the environment (humidity, light)	Light shining into the eye is relatively easy to control, light and sidelights shining on the face are relatively difficult to control (due to the scale of verification peripherals); humidity and temperature are most difficult to control, especially on airports and national borders
Measurability	Features are measurable with simple technical instruments	The proposed features are equal in this respect
PERFORMANCE IN TIME		
Permanence	Change of features over time	The iris is most stable in time, faces change due to age; fingers do change over short periods of time and sometimes disappear
Stability	Change of features due to changes in circumstances	Faces are influenced by emotions, fingers and iris are not; but fingers maybe cold or warm, sweaty or dry due to emotions, thus influencing liveness detection and causing false rejections
FRAUD RESISTANCE		
Copy proof	Live features are difficult to copy	If a biometric identity document is available, it is very easy to make a copy of the digital image of face, iris and finger; if no document available, it is relatively easy to take a picture of a face, to copy a fingerprint left on a glass is less easy; to make a picture of an iris, the subject has to co-operate to a certain extent
Spoof proof	Features are difficult to spoof	It is easy to spoof a fingerprint (using film) [37]; to spoof an iris is less easy or more costly (lenses); a spoofed (3D) face (mask or heavy make up) is difficult to hide
Liveness detection	Ability to detect liveness of feature	It is easy to detect a lack natural movements of a face; liveness detection of iris and finger are not well developed and are easy to fool [26]

PUBLIC ACCEPTANCE		
User friendliness	Easy and comfortable to measure	Finger is often perceived to be most simple and user-friendly
Cultural factors	Willingness of the public to show feature; religious or cultural groups should not be excluded as a whole	Showing a face or the touch of a finger are taboo in some cultures, this might lead to a lack of co-operation by partial covering of the face or pressing a finger or even refusing to show the feature at all; Orthodox Muslim women for example are unwilling to show their face at all, for this group, face recognition technology is not an option; Some people might be reluctant to show their iris because they fear that information about their health is leaking out of the system

I evaluate each type of biometric feature against these factors. First, I assign a relative weight to each factor. Next, I assign an evaluation of this factor, related to face, iris and fingerprint technology.

The ranking varies from 0 to 10. The results of this evaluation are included in Appendix 2.

The assignment of a relative weight to a particular factor is of course of a subjective nature.

This is due to the fact, that we have, for example, no exact information on the target group. For example, we probably can estimate how many orthodox Muslim women are part of the target group. But we cannot predict how these women will behave. We have no experience with biometrics in a multicultural context. And if we would know that people do not refuse to show their face *today*, we do not know how many people would or would not refuse to show their face *tomorrow*.

It is up to policymakers to decide whether it is important to anticipate on this issue. If policymakers judge that it is very important to include all cultural groups, they may (subjectively) decide to assign the highest weight of 10 points to the factor ‘culture’.

People might also refuse to show their eyes, because they fear that information about their health is leaking out of the system. This problem might be solved legally, by forbidding the use of information as a proof of health.

The weight of the factors ‘permanence’ and ‘stability’ depends fully on the aimed application. If we want a stored biometric feature to be valuable over time and circumstances, a high weight is to be assigned to these factors.

If policy makers decide to implement strong supervision, attempts to spoof biometric features will be detected, in most cases. The weight assigned to the factor ‘spoof proof’ will then be low. Thus, although the evaluation of a particular biometric technology for this factor might be low, this will not have a heavy impact on the overall evaluation of this technology. Of course, supervision should be equally strong in the identity document chain.

The evaluation is not definitive. A number of factors, which can be measured, for example ‘liveness detection’ and ‘spoof proof’ have not been exposed to large-scale practice. It is useful that experts on biometric technology correct my evaluation of the respective factors. Also, these factors are to be monitored and the evaluation is to be adapted over time.

I do not intend to generate absolute answers to absolute questions. Rather, the evaluation instrument I developed is a starting point and may serve as a strategic instrument, helping policymakers to take the right decisions.

From my evaluation follows that:

1. In general, iris technology scores best followed by finger technology. If the scores are weighted, face technology is second best. However, the distance between the scores of this technology is low in both cases.

2. The ability to enrol is the highest in face technology, followed by iris technology.

3. The actual performance of iris technology is the best; finger technology is second best. The performance of face technology is significantly lower.

4. Iris technology also scores best for permanence in time. The distance between the scores of finger technology and face technology in this respect is low.

5. The score for fraud resistance of iris technology is highest, followed by face technology. The fraud resistance of finger technology appears to be very low.

6. The scores of finger technology for public acceptance are highest; the scores of iris technology are just below the scores of finger technology. Face technology scores significantly lower.

CONCLUSIONS CHAPTER 8

<Sub conclusion 8.1> Performance criteria for supervised passage are arbitrary and need to be reconsidered. In doing so, we have to take into consideration
1. the low performance in groups of look alike frauds
2. the percentage of fallback procedures we are willing to accept

<Sub conclusion 8.2> The impact of race, sex, age and psychology is lowest on iris technology.

<Sub conclusion 8.3> The actual performance of iris technology is the best; finger technology is second best. The performance of face technology is significantly lower.

<Sub conclusion 8.4> Iris technology also scores best for permanence in time. However, the distance between the scores of finger technology and face technology in this respect is low.

<Sub conclusion 8.5> The score for fraud resistance of iris technology is highest, followed by face technology. The fraud resistance of finger technology appears to be very low.

<Sub conclusion 8.6> Iris technology performs best on groups of look alike frauds. Further research is necessary in order to find out whether iris technology is a suitable instrument to fight look alike fraud.

<Sub conclusion 8.7> The ability to enrol is the highest in face technology, followed by iris technology.

<Sub conclusion 8.8> The scores of finger technology for public acceptance are highest; the scores of iris technology are just below the scores of finger technology. Face technology scores significantly lower.

IV - STRATEGIC CONSIDERATIONS

CHAPTER 9 – BIOMETRICS IN NATIONAL IDENTITY MANAGEMENT

THE LOGIC OF IDENTITY DOCUMENTS

Keys are instrument to get access to a logical or physical domain.

Keys *grant access* to logical or physical domains. Characteristics of a *true* key are *secrecy*, *randomness* and the *ability to update or destroy*. A key is a *constant*. A key contains no explicit information on the key holder or on the domains, premises or closets to which it gives access. Keys are not necessarily common across functions (Bruce Schneier, [28]).

National identity documents are used as keys.

National identity documents *grant access* to physical domains, e.g. to countries as well as to logical domains, e.g. to public and private services.

Secrecy of national identity documents

Travel documents are difficult to copy or forge. A number of visible and invisible features, e.g. watermarks and holograms, protect the national identity document against forgers.
Part of the security marks of travel documents, are *secret*. Driving licences are easier to copy and do not contain secret security marks. In this respect, a travel document is a *true* key, a driving license is not.

Nevertheless, it is the intention of the government to prevent that illegal copies of national identity documents are made by keeping the 'recipe' *secret*. Like door keys, national identity documents can be stolen and abused. However, even stolen keys do open doors.

Randomness of national identity documents

National identity documents are nor random but based on a number of characteristics of the document holder, both visual (picture of the face) and textual (name, date of birth). In this respect, national identity documents are not *true* keys.

Ability to update or destroy national identity documents

National identity documents can be destroyed, both physical and logical, by putting them on an black list. They also can be updated, i.e. replaced, the old document is either physically destroyed, if available, or logically destroyed, by putting it on a black list.

Not all authorities will check a black list during the identification process. Thus, the logical destruction of a national identity document is only partial: in certain domains or on certain occasions it will still be possible to use a national identity document after it has been logically destroyed. In this respect, a national identity document is only to a certain degree a *true* key.

Contrary to keys, national identity documents contain explicit information about the key holder.

The identity document contains printed and digital information
1. on the attributed identity of the document holder e.g. name, date and place of birth, social security number etc.; and
2. on the biometric identity, i.e. a photograph of the document holder.

Thus, an identity document is to be compared with a key with a labelled key, the label tells to whom the key belongs. The identity information printed on the document may act as a starting point for identity theft.

The social security number links the document to the fiscal domain and the domain of social security. The authorities in charge reason that if the document is genuine, the social security number must be genuine as well. Due to this, the social security number is 'trusted by definition' and frequently used as a unique identifier in these and other domains.

Thus, the printing of the social security number on the national identity document induces feature creep: as a consequence, the social security number is used as a unique identifier, a function the social security number was never designed for.

Contrary to keys, national identity documents contain implicit information about the premises to which it gives access.

Not printed on the document, but publicly known, are the physical (e.g. countries) and logical (e.g. public and private services) domains to which the national identity document gives access. The domains, to which the national identity documents give access to, are publicly known.

In other words, national identity documents are comparable to keys under the doormat.

THE LOGIC OF BIOMETRICS

Biometric features are not keys

As pointed out before, face, iris and finger are public biometric features and thus *not secret*: they are easy to access and to copy or imitate. Once corrupted, biometric features are *not updateable* or *revocable*. Biometric features are not *random*. In addition, biometric features are necessaryly common across functions. In 'Biometrics: Uses and Abuses' [28], Bruce Schneier points out that for this reasons, biometrics are not to be compared with keys.

Furthermore, Gaël Hachez, François Koeune and Jean-Jacques Quisquater point out that, contrary to keys, biometric features, are *not constants* [5]. However, because of the similarity to keys, biometric features should be protected.

The government intends to apply biometrics on national identity documents in order to *verify* whether the document *bearer* is actually the legitimate document *holder*. In other words, the *authenticity* of the identity claim is established. Once the authenticity of the identity claim is established, the bearer can dispose of the identity document as if he or she where the legitimate holder.

Thus, biometric technology is applied to grant or deny access to an identity document, which in turn grants access to a number of physical and logical domains. In a way, biometric technology serves as a lock on identity documents and the biometric feature of the document holder serves as a key to this lock.

In other words, biometrics on national identity documents are to be considered as a key on to a key.

It is the intention of the government to apply biometrics only during supervised border passage, which means that, besides the check of biometric features, additional checks are made as well. Thus, biometrics are not the only key. In non-supervised situations, or in situations where authorities are tired of performing additional checks, biometrics will serve as the only key.

CONCLUSIONS CHAPTER 8

< Sub conclusion 9.1> National identity documents are not keys but the government treats them as such.

< Sub conclusion 9.2> An identity document is to be compared with a key under the doormat, the doormat telling a silent story about the lock the key fits in.

< Sub conclusion 9.3> National identity documents contain a lot of additional information on the identity of the document holder. The additional information may serve as a starting point for identity theft.

< Sub conclusion 9.4> The fact, that the social security number is printed on the national identity document, causes feature creep. Because of the fact, that the social security number is printed on the national identity document, it is used as a unique identifier, a function for which the social security number was never designed.

< Sub conclusion 9.5> Biometric features are not keys, but indirectly they are used as such, they serve as a key to an identity document.

< Sub conclusion 9.6> There is a risk that biometrics, in daily practice, will be treated, as the sole key during border passage. This is an instance of feature creep: the biometric feature is used as travel ‘document, a function for which it was never intended.

CHAPTER 10 – RISKS ATTACHED TO THE APPLICATION OF BIOMETRICS IN NATIONAL IDENTITY MANAGEMENT

The application of biometrics is to be evaluated in the context of *the national identity document chain* as a whole. A pro-active approach of risks is necessary in order to prevent fraud.

In the following paragraphs, I will formulate a pro-active and integrated risk approach.

ATTACKS AND ATTACK SCENARIO'S

It is useful to discriminate between attacks and attack scenarios.

Attacks are attempts to break into the biometric system, to cause the system to malfunction or even to destroy the system as a whole. But to frauds, attacks are steps, which they may take in pursuing a particular goal.

In order to achieve a goal, a fraud combines these technical attacks with other steps in an *attack scenario*.

TYPES OF ATTACKS

On public and private biometrics

As mentioned before, the biometric features proposed by the government are public, which means that they are easily stolen and copied, and may be used for spoofing and identity theft.

Once stolen, biometric features remain stolen. A pin code is easily changed; a biometric feature is not.

Contrary to the theft of a document, the theft of a biometric feature may go unnoticed, giving the fraudulent user plenty of time to take advantage of it.

The national identity document as intended by the Dutch government will contain the image of the biometric feature. The image of the biometric feature is easy to copy, and can be used for spoofing the live biometric feature. The document can be revoked logically by putting it on a black list. The biometric feature can't be revoked.

Thus, the use of public biometric features in national identity management and the fact that these features are stored on the document in the shape of an image makes the solution as a whole vulnerable to attacks.

In the digital and analogue domain

The analogue domain comprises every non-digital aspect of national identity management, such as procedures, physical facilities, personnel and production facilities. Attacks are relatively easy in the analogue domain.

Attacks in the digital domain generally require more resources (time, money, skills, information) that attacks in the analogue domain and difficult perform by individual frauds.

I will give an overview of technical attacks in the national identity document infrastructure. I will limit the risk analysis to the analogue domain.

TYPES OF ATTACKERS

Attackers may be individual frauds, brokers, saboteurs and terrorists

Individual identity frauds

Individual frauds usually attack the national identity management for their own individual benefit. They themselves aim to get access to a country or to a public or private service.

The means of individual frauds are limited. They do not have resources to break into the digital domain. They will aim to commit look alike fraud by using spoofs or by circumventing the verification procedure.

Identity fraud brokers

Brokers work on behalf of groups of individual frauds or groups of saboteurs and terrorists. Brokers are often closely linked to organised international crime and human trafficking. International crime is many instances closely linked to terrorism.

Brokers have resources to break into the analogue domain on a large scale, as well as to break into the digital domain.

Saboteurs and terrorists

Groups of saboteurs and terrorists may aim to disable the system as a whole.

They may aim at a complete deregulation of public life and probably abuse the deregulation as such for malicious purposes. Alternatively, they may take advantage of relatively weak fallback procedures during a period of deregulation.

They may also aim to pervert and abuse the system from within, either to get control over the system or to offer 'identity services' to their members.

ATTACKS

Overview of attacks on biometric processes

The publications of Umut Uludag and Anil K. Jain "Attacks on biometric systems: a case study in fingerprints" [34] and Lisa Thalheim, Jan Krissler, Peter-Michael Ziegler "Body check: biometrics defeated" [39] offer an overview of possible attacks on biometric processes. Attacks are described on the process, live and stored biometric features as well as the technical infrastructure.

Attacks on biometrics in the national identity infrastructure

An inventory of possible attacks is to be found in Appendix 3.

A schematic representation of the biometric processes in the national identity infrastructure including possible attacks is to be found in Appendix 4.

The explanation of the attacks, included in this schematic representation of the biometric processes in the national identity infrastructure, is to be found in the following table.

This is followed by a description a couple of attacks in particular.

Table 15 – Attacks on biometric processes

	Domain					
		Digital				
	Analogue	Storage	Transmission	Devices	Link biometrics - id	Description
Verification	1					Manipulate biometric registration (frustrate process, mutilate or spoof biometric feature)
			1			Manipulate or intercept data transmission
				2		Manipulate sensor
			3			Manipulate or intercept data transmission
				4		Manipulate feature extraction
			5			Manipulate or intercept data transmission
				6		Manipulate matcher (process, operating point)
			7			Manipulate or intercept data transmission
	8					Circumvent decision
			9			Manipulate or intercept data transmission
	10					Manipulate or steal identity data stored on document
		11				Manipulate or steal biometric data stored on document chip
					12	Manipulate the link between identity and biometrics stored on document (insert new chip, use external chip)
			13			Manipulate or intercept data transmission
Enrolment			14			Manipulate or intercept data transmission
				15		Manipulate sensor
			16			Manipulate or intercept data transmission
				17		Manipulate feature extraction
			18			Manipulate data transmission
		19				Manipulate biometric data stored in database
					20	Manipulate the link between identity and biometrics stored in database (insert new biometric data)
		21				Manipulate identity stored in database
			22			Manipulate or intercept data transmission
	23					Manipulate biometric registration (frustrate process, mutilate or spoof biometric feature)

Explanation of some attacks on biometric processes

Attackers may fool biometric technology by spoofing. In this way, an individual fraud can arrange to be falsely accepted.

Attackers may circumvent the decision of biometric technology, by joining somebody else, who was accepted, through the gate.

An attacker may present another biometric feature to the sensor, i.e. a biometric feature stored not stored on the identity document but on another chip. In this way, a false acceptance is guaranteed.

By manipulating the system operating point, an attacker can arrange for many frauds to be falsely accepted.

An attacker may deliberately mutilate his or her biometric feature before enrolment, thus preventing authorities to insert a biometric feature on the identity document. In this way, the attacker can enforce the use of fallback procedures. An old fashioned non-biometric document is an interesting trade-object as well.

ATTACK TREE ANALYSIS

As said before, frauds combines technical attacks with other steps in an *attack scenario* in order to achieve a particular goal.

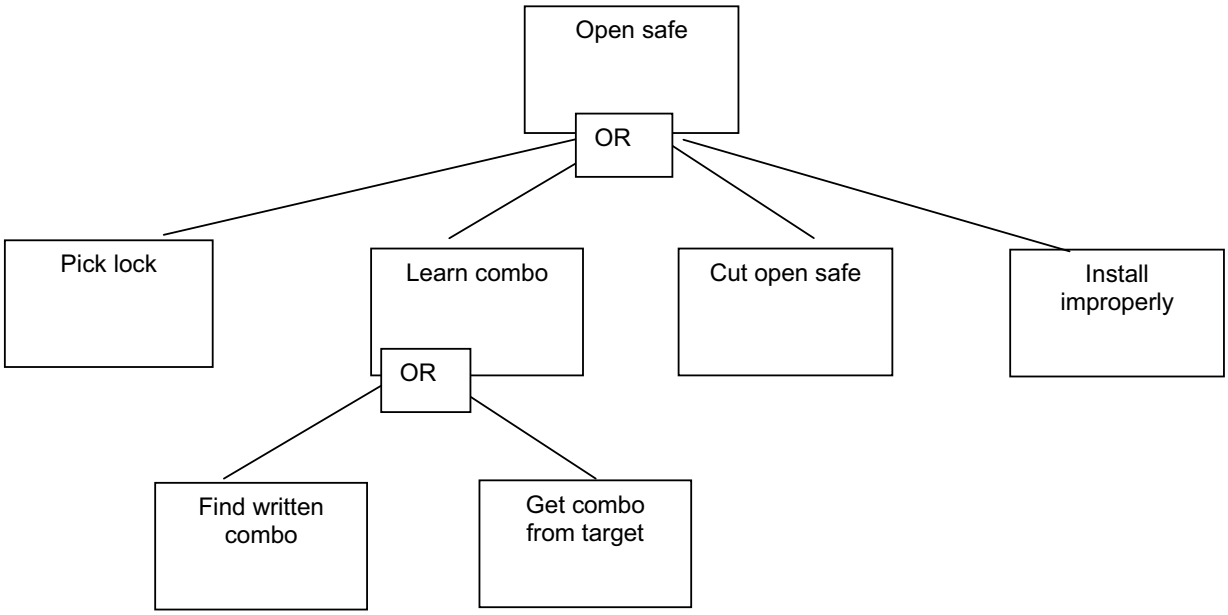
The method method of attack tree analysis, developed by Bruce Schneier offers a framework to analyse these attack scenario's [29]. Attack trees analysis provides a formal, methodical way of describing the security of systems, based on the intention of the attacker and a range of possible attacks.

Attacks against a system are represented in a tree structure, with the goal or intention of the attacker as the root node and different steps of achieving that goal as leaf nodes. A collection of leaf nodes, attached to one node constitutes a branch. A particular tree can serve as a branch in one or more other trees.

A graphic representation of attack trees

Below, for instance, is a simple attack tree about opening a physical safe. The goal of the attacker is opening the safe. To open the safe, an attacker can pick the lock, learn the combination, cut open the safe, or install the safe improperly so that he or she can easily open it later. To learn the combination, he or she either has to find the combination written down or get the combination from the safe owner.

Figure 2 –A graphic representation of an attack tree: 'open safe'



OR nodes and AND nodes

In this example, OR nodes are included, which means the attacker has a choice between different steps in order to achieve the goal. If all steps are to be performed in order to achieve the goal, an AND node is to be included in the tree. For example, in order to eavesdrop on someone saying the safe combination, attackers have to eavesdrop on a conversation AND get safe owners to say the combination. Attackers can't achieve the goal unless both sub-goals are satisfied.

Weight of steps

Values or 'weights' can be assigned to the steps in order to indicate the relative effort necessary to perform a step. Factors determining the relative weight of a step are:

1. Difficulty
2. Expensiveness
3. Lawfulness
4. Equipment needed
5. Intrusiveness
6. Probability of success
7. Likelihood the attacker will try the step
8. Risk of being catched
9. Risk of being detained
10. Risk of being killed

OR nodes have the value of their cheapest child; AND nodes have the value of the sum of their children.

Research on the target of attack is necessary in order to assign these quality values to the nodes of an attack tree.

Different types attackers have different levels of skill, access, risk aversion, money, and so on. Attackers, too, have to be evaluated against the qualities mentioned above.

Note that the effort needed for a particular step may even encourage an attacker and establish a sub-goal in itself. A tramp, for example, might be longing to go to jail. A terrorist may dream of dying and becoming a martyr. This averse attitudes of attackers turn the attack tree inside out.

Once the weights of the nodes are established against the particular qualities, the tree can be used to determine the vulnerability of a system for a particular type of attacker.

If, for example, the costs attached to the performance of a three are lower than the budget of the attackers against whom we want to protect the target, the target is exposed to a serious threat.

Abstract representation of attack trees

Schneier chooses to represent attack trees in a graphic shape. In this way, the trees are easy to grasp. Graphic representations however are difficult to model. For this reason, I developed an abstract representation of attack trees. I programmed the boolean nodes (and / or) in an exel sheet. Steps and the values or weights attached to these steps are defined centrally, in order to make a 'system wide' modelling possible.

ATTACK SCENARIO'S: MULTIPLE IDENTITIES, LOOK ALIKE FRAUD AND IDENTITY THEFT

A primary intention with the application of biometrics in national identity management is to fight *look alike fraud*. It is worthwhile to evaluate the effectiveness of biometrics against look alike fraud.

Identity theft is rapidly becoming a major crime [51]. Identity theft incidence rates have accelerated, impacting over 27 million Americans in the five-year period 1998 to 2003, according to the Federal Trade Commission analysis. It is only reasonable to assume that identity theft is a threat to national identity management in general.

Multiple identities do occur, and are abused for criminal purposes [23]. We do not know exactly to which extent. Names of foreigners are frequently misspelled and the errors in the registration of foreigners are 'exported' to national population records, thus giving birth to 'multiple identities'. Because population records are distributed over municipalities, these multiple identities often go unnoticed. Of course, names can also be misspelled on purpose by frauds in order to create multiple identity.

For the actual attack scenario analysis of these types of fraud, see Appendix 5.

RESULTS OF ATTACK TREE ANALYSIS

General results

To pretend a false rejection is an attractive escape route for a fraud, both when genuine or spoofed biometric features are used. This stresses the importance of a strong fallback procedure.

Standard identification procedures, including biometric verification, are highly predictable and thus frauds are optimally prepared to pass these procedures.

It is therefore important that the FAR of the biometric system is set at a minimum value, in order to discourage frauds from trying to mislead the system. Fallback procedures should be unpredictable in order to prevent frauds to effectively prepare for it.

Spoofing of biometric features is relatively easy, due to the fact, that an image of the biometric feature is contained in the document.

The analysis is to a high degree based on assumptions on the relative difficulty of the steps to be taken in each scenario. Further forensic research is needed in order to make a more reliable analysis.

The difficulty of steps depends, among other factors, on the type of attacker. In order to mitigate risks effectively, it is important to establish a set of profiles of attackers and clearly define against which type of attacker we seek protection.

Effectiveness of biometrics against look alike fraud

Look alike fraud is still relatively easy. If a genetically related fraud uses his or her own biometric feature, a fraud might choose just to try and see if it works. For non-related frauds, it is simple to spoof the biometric feature, as the document contains the image of the biometric feature as a starting point.

Effectiveness of biometrics against multiple identities

Multiple identities are also still relatively easy to create. If a fraud wants to purchase multiple identity documents, there is no need for spoofed biometric features and he or she can resort to relatively easy, proven fraud strategies in the analogue domain. No matter whether his or her own personal records, or somebody else's, are printed on the document. Multiple

identities are difficult to trace, due to the distributed storage of population records. If centrally stored, biometrics can be used to detect multiple identities.

Effectiveness of biometrics against identity theft

The easy way to commit identity theft is to steal an identity document. Based on the biometric and personal data it contains, it is still not too difficult for a fraud to obtain a fresh but illegitimate identity document. Personal and biometric features are included in the document.

CONCLUSIONS CHAPTER 10

<Sub conclusion 10.1> In order to assess risks properly, attack scenario's and attackers are to be evaluated. In addition, further forensic research on the difficulty of attacks is necessary.

<Sub conclusion 10.2> Public biometric features are vulnerable to attacks. They are easy to steal and copy, and, once stolen, they remain stolen.

<Sub conclusion 10.3> The storage of image of the biometric feature on the document serves as a 'fraud toolkit', containing the crucial ingredient for spoofing.

<Sub conclusion 10.4> Standard procedures for identification are highly predictable and enable frauds to be optimally prepared and successful.

<Sub conclusion 10.5> Fallback procedures deserve special attention, as they are probably abused in order to circumvent a negative result of biometric verification. A fallback procedure should never be an attractive alternative for frauds.

<Sub conclusion 10.6> A high FAR renders a biometric system ineffective.
Thus, the operating point of biometric systems needs to be operated and managed in a secure manner.

<Sub conclusion 10.7> In order to detect and fight multiple identities, the storage of population records, or at least the storage of biometric features, is to be centralised.

<Sub conclusion 10.8> Look alike fraud, multiple identities and identity theft are still not too difficult after biometrics have been applied on national identity management. The effectiveness of biometrics against these fraud scenario's depends on the degree to which the problems mentioned above are solved.

CHAPTER 11 – RECOMMENDATIONS

BIOMETRIC TECHNOLOGY

Use private biometric features

The type biometric features, as proposed by US and EU authorities, is *public*, which means they are easy to steal and abuse. Compromised biometrics, are compromised forever and can not be revoked.

Instead, it is advisable to use *private* biometric features, for example, epidermal vain structures.

Use randotypic biometric features

Face and finger are to a high degree genotypic biometric features, which means they are ineffective as an instrument against look alike fraud.

Instead, it is advisable to use *randotypic* biometric features. The iris is randotypic. Epidermal vain structures are probably pure randotypic as well, though I have not yet been able to verify this.

Apply combined biometrics

A low FAR is a critical criterion for success. Thus, it is important to improve the overall performance of biometric technology. In 'Multimodal biometrics': an overview' [53], Anil K. Jain, A. Ross and A. K. Jain describe that combined biometrics might yield performance improvement of a factor of 2 – 10, strong technologies benefit more and might achieve even a higher performance.

Combined biometrics also partially mitigate the risk of spoofing biometric features. Although it is possible to spoof two biometric features successfully, it is certainly much more difficult to do so *and* pass the verification procedure.

It is advisable to apply *combined biometrics* both in order to achieve a better performance and to prevent spoofing.

STORAGE OF BIOMETRIC FEATURES

Store biometric features in central database

If a document contains a perfect image of the biometric feature, it offers the crucial ingredient for spoofing. The document thus serves as a 'fraud toolkit'. A Private Key Infrastructure could be used to prevent unauthorised reading of the biometric features by ascribing private keys to authorised biometric peripherals. However, this is a rather expensive and certainly very complex solution, as all peripherals all over the world are to be registered.

The biometric feature stored on the document can also purposely be damaged. During verification, frauds can pretend to be falsely rejected in order to resort to the fallback procedure.

In order to prevent spoofing and to prevent damage of the stored biometric feature, it is an option to store the biometric feature in *a central database* instead of the document. This might also prevent some frauds from claiming false rejection.

Apply matching on card algorithm

The storage of the biometric feature on the card poses a risk, because anybody can read the feature from the card. If a matching on card algorithm is applied, no biometric peripherals are

needed; instead, the card itself compares the live biometric feature with the stored biometric feature. Thus, the stored biometric feature can be read-protected.

In order to prevent spoofing, it is an option to apply a *matching on card* algorithm.

COMBINE LOGICAL PROPERTIES OF KEYS AND BIOMETRICS

Biometrics are not keys. Biometric features are *neither secret*, nor revocable or random. And they are common across functions. Thus, biometric features are not keys and should not be used as such.

However, biometrics have the potential to establish an unbreakable link between a subject and an entrance code and we would rather not loose that property.

Apply biometric keys

In 'Information-Theoretic Approach to Privacy Protection of Biometric Templates' [43], Jasper Goseling and Pim Tuyls describe a solution in which the properties of keys are combined with the properties of biometrics.

A random secret constant or 'helper data' is used to select a subset of properties from a biometric feature. These helper data can be stored on a chip. The subset of properties constitutes a *biometric key.* On verification, *the biometric key* is again reconstructed, using the 'helper data' on the chip. Variable elements are eliminated during the process. The algorithm allows for 2^{24} sets of 'helper data' which is roughly enough to allow for revocation and refreshment during a couple of reincarnations.

V - CONCLUSIONS

Conclusion 1

Fraud in general is a blind spot. The extent of id fraud is large and growing fast. Identity fraud is perceived as an external risk both by government and by citizens. The quality of population records is unsatisfactory.

The quality of national identity management is insufficient. Risks of identity fraud are not properly managed and mitigated by the government. Governments lacks a coherent vision and strategy. Improvement of national identity management is necessary to safeguard national security.

If national identity management in general is not improved, biometrics worsen the situation, which may put national security at risk.

Conclusion 2

We have no information about the effectiveness of biometrics against look alike fraud in large world-wide heterogeneous user groups. In addition, we lack information on the performance of biometrics in genetically related groups and about fraud resistance. We do not know the impact of the application of biometrics on the alertness of authorities in charge of identification.

We have insufficient information about the effectiveness and side effects of biometrics in national identity management.

Conclusion 3

No relevant data on the performance of biometrics in national identity management are yet available. This exposes citizens to risks, for example false accusation of look alike fraud or identity theft, which can be mitigated by the Dutch authorities. Use of biometric national identity documents abroad exposes citizens to risks which cannot be mitigated by their own national authorities

Mandatory application of biometrics will probably lead to circumvention of biometric procedures and enforced use of fallback procedures.

Voluntary application of biometrics in national identity management is advisable. This is in the interest of both government and citizens.

Conclusion 4

An identity document is not a key but is treated as such by the government. An identity document is to be compared with a key under the doormat and contains a lot of additional information on the identity of the document holder. Thus, the document serves as a starting point for feature creep and identity fraud.

A biometric feature is not a key, but is treated it as such in the context of national identity management. Besides, there is a chance that biometric features, in daily practice, will be mistaken for identity documents, thus causing a second instance of feature creep.

Identity documents and biometrics are not keys and are not be treated as such. The application of biometric keys is recommended.

Conclusion 5

No relevant data on the performance and effectiveness of biometrics against look alike fraud in national identity management or in large heterogeneous groups are yet available. Performance criteria for supervised passage are arbitrary and need to be reconsidered. Iris technology seems to be the best instrument against look alike fraud. In addition, the fraud resistance of iris technology is the best. Finger technology is less suitable in these respects, in particular because it appears to be not very resistant against fraud.

Within the boundaries of US and EU regulations, iris technology is the best instrument against look alike fraud. The Dutch government should withdraw from applying finger technology on national identity documents.

Conclusion 6

In order to assess risks properly, attack scenario's and attackers are to be evaluated. Forensic research on profiles of attackers and the difficulty of attacks is necessary.

National identity management should focus on attackers and attack scenario's in order to mitigate the risks attached to biometrics in national identity management.

Conclusion 7

Biometrics make national identity management more vulnerable to attacks, because of:
- The application of public biometric features (can be copied and spoofed)
- The unprotected storage of image of the biometric feature on the document (can be stolen)
- Standard procedures for identification (can be predicted by frauds)
- The variability of the operating point of biometric systems (can be manipulated by frauds)
- Relatively weak fallback procedures (can be used in circumvention of biometric procedures)
- Decentralised storage (allow undetected multiple identities)

Look alike fraud, multiple identities and identity theft are still relatively easy to perform after biometrics have been applied on national identity management.

Main conclusion

Do not apply face and fingerprint technology in national identity management. *Do not* store the image of the biometric feature on the document.

Instead,

1. Apply biometrics:
- based on private biometric features;
- based on randotypic features; and
- use combined biometric algorithms.

2. If public *biometric features* are applied, protect these against unauthorised parties through:
- storage in a central database; or
- read-protected storage on document combined with matching on card algorithm

3. Preferably, apply *biometric keys*, which combine the logical properties of keys and biometrics:
- key: secret, revocable, random, not common across functions; and
- biometrics: link between subject and key

APPENDICES

1. References
2. Influences on performance
3. Inventory of attacks
4. Risks infrastructure
5. Attack scenario's
6. EC Directive 95
7. Dutch legislation