Implications of applying biometrics to travel-documents[**]

Rudolf L. van Renesse[*]

TNO Institute of Applied Physics
P.O. Box 155, 2600 AD DELFT, The Netherlands

ABSTRACT

The Dutch government currently considers the decentralised storage of the enrolled template of the document holder on a chip embedded in the travel-document in order to allow biometric verification if the document is presented by the rightful holder. The main purpose of the intended biometric application is combating the misuse of travel-documents by look-alikes. Because travel-documents simultaneously function as identity documents, this misuse not only involves border crossing but also acquiring services from government, municipality and the private sector.
This paper recognises some inherent problems: (1) due to human factors, false reject rates will expectedly be considerable, and look-alikes will claim to be falsely rejected (2) the look-alike may sabotage the biometric functionality of the travel-document and (3) the enrolment process may be fraudulently frustrated. Partial solutions are layered biometrics and centralised storage of personalised templates in the registers of travel-documents or their semi-centralised storage in municipal registers.
The usefulness of decentralised storage of biometric templates on travel-documents is discussed.

Keywords: Biometrics, false reject rate, look-alikes, travel-documents, template distribution, processing of personal data

1 INTRODUCTION

This paper discusses the problems related to decentralised storage of biometric templates on travel-documents as a means to combat look-alike fraud. The analysis focuses on the current situation in the Netherlands, but is believed to also have international significance. The following introductory information is derived from a May 2001 letter by the Minister for Urban Policy and Integration of Ethnic Minorities in the Netherlands [1].
In the Netherlands, in 1988, the project "New Generation Travel-documents" was started and it was recognised from the start that information and communication technology (ICT) potentiality offered security enhancement of travel-documents. For that reason, in 1988, the Cabinet instructed the performance of a feasibility study for (1) the application of biometrics on travel-documents, (2) smart card technology and (3) public key infrastructure (PKI), primarily aiming at protecting travel-documents against misuse by look-alikes. Travel-documents simultaneously function as identity documents and this misuse extends from border crossing to acquiring government, municipal and private services.
Momentarily, studies of the International Civil Aviation Organisation (ICAO) have pointed at three biometric technologies that offer the most potential: facial recognition, finger pattern recognition and iris recognition. An ICAO recommendation with respect to these biometric technologies is expected in the year 2003.
As soon as international consensus is established with respect to preferred biometric technologies, the new Dutch passports, launched late 2001, can be fitted with a chip, antenna and the relevant biometric and ICT functionality. A biometric verification procedure thus allows establishing if the legitimate holder presents the travel-document. Such distributed (de-central) registration of templates only allows biometric verification (one-to-one comparison of current and enrolled template) and excludes biometric identification procedures (one-to-many search of a match for the current template in an enrolled template databases).

[**]Presented at the Conference on Optical Security and Counterfeit Deterrence Techniques IV, San Jose, CA, USA, 23-25 January 2004, SPIE Vol. 4677, pp. 290-298.
[*]Willem de Zwijgerlaan 5, 2582 ED The Hague, The Netherlands, Ruud_van_Renesse@zonnet.nl

2 LEGAL ASPECTS

Important legal aspects concerning the application of biometrics to travel-documents, recognised by the Dutch government are, amongst others [1]:

- Storage and processing of the biometric information (meant is the biometric template) must be carried out so that it cannot be considered *sensitive information*, that is, it must not contain characteristics of race, health, religious denomination, etc.
- The distribution of the biometric information (meant is the biometric template) must be prevented, on the one hand by decentralised storage in the chip, on the other hand by not storing the biometric information in files of verifying authorities during verification.

It is noted however, that the storage of the biometric template together with other personal data[1] in the registers of travel-documents is currently considered. These accounts serve consultation in case of loss and other special circumstances in the use of the travel-document [1].

In 1997 an authoritative study was published in the Netherlands on the legal aspects of the application of biometrics [2]. In this study, the authors conclude that, if the biometric template is linked to personal data, it must be also considered as personal data. Legal consequences are attached to the qualification of the biometric template as personal data. In particular, based on European directives, the Dutch Personal Data Protection Act states that it is prohibited to process personal data concerning a person's religion or philosophy of life, race, political persuasion, health and sexual life, etc.[2] However, in agreement with the European directives, the law also states that the prohibition on processing personal data concerning a person's race, does not apply where the processing is carried out with a view to identifying data subjects and only where this is essential for that purpose.
The authors conclude that currently, if a reasonable importance is at issue, in view of security, it is allowed to register biometric information in the form of templates that cannot be converted to the original biometric information (this is the complete input biometric image or signal, such as an image of the fingerprint or a voice recording). Tentatively, the authors of this study [2] assume that sensitive information cannot be derived from biometric templates because the original biometric information can no longer be derived from it. This being the case, they conclude that biometric templates cannot be considered sensitive information. If, however, biometric templates could be considered to contain reconstructible sensitive information, the authors tend to the opinion that such information cannot be lawfully registered.

It may be put forward that it would be very difficult, if at all possible, to prove that biometric templates do not carry sensitive information and without such proof it appears dubious to maintain that biometric templates in general can be trusted not to contain sensitive data. Manufacturers do not tend to give insight in their algorithms and the analysis of templates on the presence of sensitive data or secret backdoors requires independent expertness. A passport photo reveals racial characteristics as well as, in certain cases, religious denomination; faces and electrical skin resistance may reveal psychological states. If such information can be derived from biometric templates, these must be considered sensitive information. For instance, it is conceivable that biometric templates, such as facial templates or any templates that are derived of skin surface, contain data that correlate with race without requiring full restoration to the original biometric information. Expectedly, such sensitive data would not be collected on purpose, but neither are passport photos taken to the purpose of revealing racial characteristics.

---

[1] Personal data are all data that supply information about a subject or that may influence the way that this subject is judged or treated. Such data comprise name, date of birth, address, bank account, profession or car licence number. The qualification “personal data” requires that the subject in question is tracible and identifiable on the basis of this information. Personal data are *sensitive* in case they provide information on a person's religion or philosophy of life, race, political persuasion, health and sexual life, or personal data concerning trade union membership.

[2] Directive 95/46/EC of 24 October 1995 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data: Article 8 - The processing of special categories of data: 1. Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

Considering the above, centralised registration in travel-document registers or semi-centralised registration in municipal registers of biometric templates seems to be a thorny matter. It has also been put forward that such storage is unnecessary because decentralised template storage in chip cards allows adequate off-line verification [2].

However, it is shown in section 4 that the application of biometrics on travel-documents in order to protect these against misuse by look-alikes, irrefutably demands centralised or semi-centralised registration of biometric templates linked to personal data. As a consequence, the question may be raised what the use is of the storage of biometric templates on travel-documents. Additionally, the hazard involved may be mentioned: the improper use of biometric verification abroad may lead to unfounded accusations of look-alike fraud and thus expose the travel- document holders to unknown risks [3]. It must be decided who will be entitled and enabled to actually carry out biometric verifications with the use of travel-documents.

The Dutch Data Protection Authority[3] in a 1999 reconnaissance of the consequences of biometrics for privacy, has formulated eight questions as a lead for assessing the justifiability of biometric applications [4]. It is observed that these questions omit touching the problems mentioned above. In section 6 these particular questions will be dealt with and tentative answers will be formulated in the context of biometrics on travel-documents.

3 BIOMETRIC FUNCTIONAL RATES

Relevant biometric functional rates are the Failure to Enrol Rate (FER), the Ability to Enrol Rate (AER), the False Reject Rate (FRR), the Ability to Verify Rate (AVR) and the False Accept Rate (FAR).
FRR and FAR are functions of the tolerance setting of the biometric equipment. The so-called equal error rate (EER), sometimes referred to as the "cross-over rate", is given by a tolerance setting such that: EER = FAR = FRR. The EER thus is given by the cross-over point of the false accept curve and the false reject curve, but it gives no information on the gradient of those curves. It is impossible to derive essential information on two variables (FRR and FAR) from one single variable and the EER therefore is a rather useless quantity.

Enrolment - A certain percentage of people appears to have insuperable difficulties to enrol at all on a certain biometric system, a percentage that is referred to as the Failure to Enrol Rate (FER, often inconsistently referred to as FTE). The FER comprises the failure to acquire rate (FTAR) and the failure to qualify rate (FTQR).
The FTAR involves subjects that are unable to present the requested biometric (e.g. missing fingers, bandage covering biometric), while the FTQR rate concerns subjects that are unable to generate a template of sufficient quality (e.g. shallow or disrupted finger patterns). It is noted that a low FTQR does not necessarily imply a high quality biometric system. A biometric system may enrol every subject, to yield high error rates in the verification stage. On the other hand, a high FTQR system may reject the enrolment of relatively many subjects, to later yield low error rates for the qualified subject group.
The ability to enrol rate is given by: $AER = (1 - FTAR)(1 - FTQR)$.
The failure to enrol rate is obviously given by: $FER = (1 - AER)$.

Verification – During normal use, a certain percentage of users will be falsely rejected by the biometric system, a percentage that is referred to as the False Reject Rate. The FRR comprises the Failure To Verify Rate (FTVR) and the False Non-Match Rate (FNMR). The FTVR concerns those subjects that could present their biometric at enrolment, but (temporarily) do not have this ability at the moment of verification as well as cases where a signal or an image of sufficient quality cannot be captured by the biometric system. The FNMR involves subjects that are falsely rejected during verification because the system is unable to match the current biometric template with the enrolled (historic) biometric template.
The false reject rate is given by: $FRR = 1 - (1 - FTVR)(1 - FNMR)$.

[3] The Dutch Data Protection Authority is an independent supervisory authority that monitors the application of the legislation concerning the processing of personal data. The Data Protection Authority advises the government on data protection issues, gives information to the general public, hears claims concerning possible breaches of the data protection legislation, approves codes of conduct and privacy regulations and has investigative powers.

Total biometric functionality - Together, the FER and the FRR give rise to two complementary functional rates of biometric systems: the Ability to Verify Rate (AVR) [5] and the Drop Out rate (DOR).
The AVR comprises all subjects that can successfully make use of the biometric system, while, obviously, the DOR comprises those who cannot.
The ability to verify rate is given by: AVR = (1 - FER)(1 - FRR).
For small error rates, this rate is well approximated by: AVR = 1 – (FER + FRR).
The drop out rate is given by: DOR = 1 – AVR.
For small error rates, this rate is well approximated by: DOR = FER + FRR.
In the context of this paper only the DOR will be further investigated because this functional rate constitutes a crucial factor with respect to the adequacy of biometrics to thwart misuse by look-alikes.

3.1 False rejects

In the first instance, the FRR of biometric equipment is investigated under optimal test conditions and as independent of human aspects as possible, in order to procure clear insight in the performance of the equipment as such. The results of such investigations become the specifications of the biometric equipment. Although this is perfectly justifiable, it cannot be concluded that this FRR specification relates to practical applications, because various human factors such as ease of use, and the user state of mind tend to influence the outcome of biometric transactions to a large degree. Ashbourn [6] gives a lucid description of the importance of user psychology. It is important to become acquainted with Ashbourn's notion of the *user psychology index* (UPI), which is a function of four user parameters: user attitude and acceptance, familiarity of user with equipment, quality of user environment, and purport of the result for the user [6,7].

The UPI index serves as a multiplier of the user independent FRR, specified by the manufacturer of the biometric equipment. In Table 1 Ashbourn's UPI is given as a function of these four user parameters. The first row of Table 1 gives the UPI of unit value that is valid under optimal test conditions, but as further rows of Table 1 show, the real life FRR may be an order of magnitude higher.

Table 1 – Ashbourn's User Psychology Index [7]; first row: user independent UPI = 1.

Attitude	Familiarity	Environment	Result	UPI
Expert	Considerable	Relaxed	Not critical	1
Professional	Normal	Relaxed	Critical	1.25
Professional	Small	Relaxed	Not critical	1.5
Professional	Small	Relaxed	Critical	2
Disinterested	Small	Relaxed	Not critical	2.25
Disinterested	Small	Relaxed	Critical	2.5
Disinterested	Small	Awkward	Not critical	3
Disinterested	Small	Awkward	Critical	3.5
Disinterested	Small	External pressure	Critical	5
Hostile	Small	Awkward	Critical	7
Hostile	Small	Awkward	Not critical	10
Hostile	Small	External pressure	Not critical	15

The results of increasing numbers of biometric pilots appear to confirm the practical value of the UPI. The performance of biometric equipment, therefore, appears user dependent as well as technology dependent. In a 1999 report to the Ministry of the Interior and Kingdom Relations [8] it is concluded that "false reject figures of different biometric 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%."
This conclusion is based on scattered reports of biometric test results in the volumes of Biometric Technology Today since 1999, partly referenced in [8]. Recent test results on finger pattern sensors [9] and a recent NPL report [10] further sustain this conclusion. It appears that even considerably higher FRR are not exceptional. Failure to enrol rates are not

negligible and further add to biometric drop out rates. Because these reject rates appear mainly attributable to human factors, there seems to be no prospect on significant improvements by future technological developments.
It is further noted that the FRR tends to increase with decreasing frequency of use, partly due to ageing of some biometric characteristics, and partly due to users never becoming fully capable in adequately operating the equipment. On an average, the frequency of biometric equipment use connected with travel-documents will be low to medium at the very best. On the basis of the forgoing, it is expected that the DOR connected to biometrics on travel-documents will be considerable. The implications for the adequacy of biometrics on travel-documents to detect look-alikes are discussed in the next sections.

3.2 Genuine rejects

A topic that is rarely touched in the context of rejects is the complete lack of the distinction in biometric practice between false rejects and genuine rejects. Obviously the travel-document inspector confronted with a reject, has no immediate way to establish whether this particular reject is false or genuine. And, as false rejects expectedly will rather frequently occur, this constitutes an essential problem. The only way to discriminate between the two is to carry out an investigation in a fallback procedure, which procedure was recently qualified as follows [11,12]:

> "If the verification process does not proceed flawlessly, one regularly falls back on defective procedures with a high probability of making mistakes, such as visual recognition on the basis of a photo or directly deriving information from an uncontrollable or uncontrolled document. Insiders know how easily the human mind sees what it expects to see and how difficult it is to distinguish between look-alikes."

The proper operation of biometric equipment and procedures depends highly on the co-operation of its users. Obviously, if the user acquires services by being accepted and is a legitimate user, the user will tend to be co-operative. Otherwise, the user will gain nothing by co-operation and will be a non-co-operative or even a hostile user. Undoubtedly, look-alikes will belong to the latter user classes.

3.3 Biometric pilots in the Netherlands

In order to gain practical experience with biometrics, a series of small-scale biometric pilots in the Netherlands is started and planned by government institutions [1]. These pilots concentrate on the biometric technologies provisionally selected by ICAO: facial recognition, finger pattern recognition and iris recognition.
In Delft a small pilot of 50 users started 11 December 2000 offering remote Internet services by various parties in the social security sector. The participants use a smart card secured with fingerscan biometrics and a reader connected to a PC. It appears that a 6% FER was encountered [13].
A six months iris-scan pilot started in June 2001 in Rotterdam in behalf of monthly identification of foreigners at the municipal Alien Police. Participants use a contactless chip card, the enrolled iris template being stored on the chip. Identification can take place at electronic kiosks.
Another pilot, using facial recognition and a combi-card (remote/contact), was planned to start late 2001.
Schiphol airport is now running an iris recognition pilot on behalf of frequent flyers. This concerns a co-operation with the Royal Military Police and the Immigration and Naturalisation Service.
Large-scale pilots are also planned and being prepared. These pilots expectedly involve the sectors of banking, social security and labour service.
The question may arise what the relevance of such small scale pilots is for detection of look-alike applications. The pilots invariably involve user services and thus presuppose co-operative participants. However useful the results of such pilots may be, they are of little or no value to assess the prospect of a very large-scale application of biometrics to travel-documents in order to solve the look-alike problem. The latter is not a user service, contrary, it is a means to control users, the user group also comprising non-co-operative and even hostile users. It would seem difficult, if at all possible, to set up pilots that supply realistic and helpful experience in the practice of look-alike fraud. Consequently, the success of the application of biometrics on travel-documents in order to detect look-alikes seems largely unpredictable.

4 Fraud aspects

Considering the above, it is helpful to conceive the various possible approaches that look-alikes may consider in order to beat the biometric system. The fact that a considerable DOR may be expected to begin with, comes to the aid of the look-alike. This may cause the look-alike to try a zero-effort attack or even to try to sabotaging the biometric system.

4.1 Zero-effort attacks

Look-alikes – their chances of being falsely accepted in a verification procedure expectedly being extremely small – have an interest in making use of possibly less adequate fallback procedures and, in such a case, will benefit by being rejected by the biometric system. This involves a zero effort attack, irrespective of the level of co-operation, where the subject inevitably proceeds to the existing fallback procedure. The obvious tactic of the look-alike is maintaining to be falsely rejected. It is impossible to distinguish between false and genuine rejects if no further verificatory means are available. This zero effort approach may additionally be supported by forcing a failure to verify that seemingly cannot be helped by the subject, for instance by mutilation of the relevant biometrics and/or having it in bandage.
The implementation of an independent second biometric would be a partial solution. The application of two independent biometric techniques is referred to as *layered biometrics*. The indicated operation mode (OR mode) is to accept a subject if either one of his biometrics is successfully verified. In this operation mode the resulting FRR considerably decreases while the resulting FAR only slightly increases[4]. Consequently, the probability of both biometrics of a legitimate user being falsely rejected is very small. A rare double reject thus points at a look-alike with some precision and warrants strict measures in fall back.

4.2 Sabotage of the biometric functionality of the travel-document

The above analysis is based on the functionality of the travel-document biometrics being fully intact. If a hostile user sabotages this functionality, the historic template is unavailable and biometric verification becomes impossible at all. Obviously, various methods, that need no further explanation, can be thought up to sabotage the biometric functionality of the chip in an inconspicuous or unsuspected manner. Because the chip-functionality on travel-documents will sometimes be lost due to production flaws or rough (or even normal) use, it cannot be concluded beyond doubt that dysfunctional chips denote fraud.
The only countermeasure against this attack is the registration of personalised templates in a centralised travel-document register or a semi-centralised registration in municipal databases. Personalising may be accomplished by linkage of the biometric template to the document number, a social security number or any suitable file number. In case of failure of the document's biometric functionality, the holder biometrics can be verified against the available database.

4.3 Sabotage of the enrolment procedure

Apart from physical sabotage of the biometric functionality of a travel-document, sabotage during enrolment must be considered. Advanced biometric equipment tests for template quality during enrolment and rejects low quality readings. Practice teaches that a certain percentage of subjects can never successfully be enrolled to biometric systems. It is noted that the respective failures to enrol add up in the case of layered biometrics and may become considerable. Expectedly, fraudulent subjects will go to great lengths to frustrate the enrolment procedure. Enrolment failures may be forced by wrongly presenting, obscuring or mutilating the biometric concerned. Finger patterns may be worn off, faces may be almost fully covered with beards or be mutilated and in bandage, artificial irises on contact lenses may be presented, etc. It may become difficult, if at all practically possible to establish whether failures to enrol are fake or genuine. Inevitably, numerous "non-biometric" travel-documents will have to be issued[5]. A solution must be found to allow making a secure distinction between biometric and non-biometric travel-documents in order to prevent the unnoticed conversion of one into the other.

4.4 Fall back procedures

If layered biometrics is applied, the chances of the look-alike making a successful zero-effort attack become slim. However, the probability of a false double reject is not zero and it is therefore desirable to have additional (administrative) verificatory measures in place. Fallback procedures in case of repeated biometric reject or dysfunction of travel-documents will depend on the requested service. The following scenarios can be tentatively conceived:
Border crossing and government or municipal kiosk services – The application of layered biometrics and access to (semi-)centralised template databases is assumed. In the case of successively failing initial verification by both

[4] In an OR mode the separate false reject rates multiply, while the separate false accept rates only add. For instance, two independent biometrics, each having a FRR of 2% and a FAR of 0.1%, together would have a FRR of only 0.04% and a FAR of 0.2%.
[5] If it is assumed that the FTE only amounts 0.1% this means that in the order of ten thousand non-biometric travel-documents for the population in The Netherlands must be issued. In practice the FTE rate may be an order of magnitude higher.

biometrics, a supervised verification is conducted in fallback, eventually connecting to on-line databases in case of chip dysfunction. If the layered fallback verification fails, a meticulous follow-up investigation is carried out.
Government and municipal remote services via PC – The application of single biometrics is assumed. If the initial verification fails, the requested service is denied and the customer is subsequently invited to apply to a counter for fallback service. At the counter dual biometrics will be available as well as access to (semi-)centralised template databases. If the fallback verification fails, a meticulous follow-up investigation is carried out.
Private financial transactions via kiosk or remote PC – Layered biometrics may be applied or not, depending on the cost involved. No access is available to (semi-)centralised template databases. If the initial verification fails, the requested service is denied and the customer is subsequently invited to apply to a counter for fallback service.
Transactions at the counter – It is conceivable that subjects are required to present biometric proof in the case of at the counter transactions, such as car rental transactions. Layered biometrics may be applied or not, depending on the cost involved. No access is available to (semi-)centralised template databases. If the initial verification fails, the requested service is denied and no fallback is available. This is an unacceptable discriminatory side-effect. Consequently, the application of biometrics for at the counter transactions with private organisations that have no access to (semi-) centralised databases will remain useless.

5 THE USEFULNESS OF BIOMETRICS ON TRAVEL-DOCUMENTS

In order to guard against misuse of travel-documents by look-alikes at border crossing, it appears necessary to take two separate measures: layered biometrics and (semi-)centralised registration of personalised templates. The first measure must be taken to counter the considerable drop out rate that is expectedly attached to a single biometric technique. Additionally, semi-centralised registration of personalised biometric templates is inevitably required in order to deal with the imminent risk of chip dysfunctionality or functionality sabotage.
Given the fact that some type of personalised template registration must take place, the question arises what the use is of having the templates also registered on travel-documents, because a subject that crosses a border can undergo a biometric verification without having his historic template stored on his travel-document anyway.

Look-alike fraud is not limited to border crossing, it is also a threat in connection with government and municipal services and transactions in the private sector. It may be assumed that government and municipal authorities also have access to semi-centralised registration of personalised templates and thus would not require template storage on the travel-document. General services mainly comprise applying for a passport, driving licence or birth certificate, remote voting and giving notice of a birth. On the average, the user frequency of such services will be low: in the order of once or twice a year, but probably less. As a consequence, false reject rates will rise accordingly. Otherwise, the usefulness of a remote service that is required with such a low frequency may be questioned.
Special govemment or municipal services may also be rendered in the social security sector. In this case the user frequency is considerably higher, but the user group is very limited and this application does not require the nation-wide implementation of biometrics on travel-documents; the issue of a special document for this service may suffice.
It is assumed that the private sector cannot revert to centralised registrations of personalised templates and thus would require the inclusion of the template in the travel/ID-document (section 4.4). Apart from the question if a biometric functionality on government issued travel-documents should be mainly there to sustain services in the private sector, the question may be raised if the private sector is ready for biometrics. A world wide feasibility study on the perspective of biometrics in the financial industry proves that this sector will not be ready for biometrics in the near future. An important objection against the application of biometrics in the banking sector appears its unacceptably high drop out rate and, moreover, there is still an international commitment towards using smart cards with a PIN [14].

It would seem evident that obligatory implementation of biometrics on all travel-documents is required, because implementation on a voluntary basis would undermine the very purpose of look-alike fraud combat. However, it is sometimes observed that even voluntary application of biometrics to travel-documents entails a certain advantage because biometric passport holders will use the biometric entry gates and no longer require the attention of the controlling authorities. Thus, more time is available to devote attention to (1) biometric rejects, (2) non-biometric documents and (3) holders of biometric documents that do not make use of the biometric gate. These groups comprise the look-alikes. Obviously, a suchlike approach reduces the biometric system to a collateral tool in the context of look-alike detection. Look-alikes will not be discovered due to the biometric system, they merely run the risk of increased attention.

6 DISCUSSION AND CONCLUSIONS

The whole concept of applying biometric technology to combat look-alike fraud is based on the underlying idea that biometric verification is superior to visual comparison of passport photographs with the face of the holder. The truth of this idea is questionable considering the error rates caused by human factors and the resulting possibilities of various types of fraud. At best the biometric application in view offers an additional tool in conjunction with human inspection. The drawbacks mentioned could be partly countered by the application of layered biometrics and the (semi-)centralised registration of biometric templates. These measures, however, do not solve the problem of enrolment fraud and the resulting issue of numerous "non-biometric" travel-documents. Furthermore, (semi-)centralised registration of personalised templates appears to remove the necessity of decentralised on-chip storage. Additionally, on-chip storage of templates entails the hazard that improper use abroad exposes the passport holders to unknown risks unless the use of the biometric functionality is restricted to authorised bodies.
Considering the above, there seems much to be said for abandoning the idea of decentralised registration of biometric templates on travel-document chips. The only advantage is that the verification process can take place off-line and thus may be faster. However, (semi-)centralised registration of personalised templates entails its own problems. It is not at all unthinkable that hackers will be able to corrupt these databases or add personalised templates to them unless efficacious security measures are taken.

As mentioned earlier, the Dutch Data Protection Authority, in a 1999 reconnaissance of the consequences of biometrics for privacy, has formulated eight questions as a lead for assessing the justifiability of biometric applications [4]. Using the results of the current analysis, tentative answers to these questions are formulated below, in the context of the application of biometrics on travel-documents. It is observed that these questions do not enter into the problems of user-fraud. Particularly, the consequences of fraud made possible by the failure to enrol rates and false reject rates attached to all biometric techniques, deserve more attention.

1. What information is actually required for the purpose?
   Personalised biometric templates registered in (semi-)central databases for the purpose of on-line biometric processing in the verification mode.
   This application significantly transcends the storage of biometric templates together with other personal data in the registers of travel-documents to serve consultation in case of loss and other special circumstances in the use of the travel-document.
2. Is the information lawfully collected? Is the person concerned informed?
   The laws concerned must be adapted [1,2]. The purpose of the biometric application must be clearly stated on the travel-document [1].
3. Is sensitive information ("special categories of data") involved?
   A well-founded answer cannot be given in general. It is insufficient to state that the original biometric information cannot be reconstructed from the template. It is conceivable that sensitive data can be derived from some templates without full reconstruction of the original information. The question must be answered if convincing à priori proof of the contrary must be provided.
4. What happens with the original biometric information? Is this deleted?
   The original biometric information is not essential for the purpose of biometric verification and should be deleted after each transaction. Convincing proof must be provided that this deletion is actually carried out and that controlling authorities will not build biometric databases.
5. Is the biometric information stored so that the original information can no longer be derived from it?
   Biometric templates expectedly do not allow full restoration of the original information. Biometric verification does not require the original biometric information and benefits by reducing the amount of information to the minimum required for adequate operation (the biometric template). Also see question 3 and 4.
6. Is a decentralised measurement and verification possible?
   A restriction to decentralised measurement and verification (using the template on a travel-document chip) is not possible for the application in view without undermining its very purpose. Centralised or semi-centralised registration of personalised templates is required to cope with sabotage.
7. Are the templates sufficiently secured?
   Because (semi-)centralised registration of personalised templates is required, databases as well as on-line transport of personalised biometric templates over information lines must be secured. As a consequence, security requirements are expectedly considerably more complex than those attached to decentralised on-chip storage.

Security requirements and measures respecting the complete IT system must be formulated, preferably according to the formalism offered by Common Criteria [15] in order to allow adequate evaluation of the system concerned.

8. Does the purpose justify centralised registration of the biometric information?
   Centralised or semi-centralised registration of personalised biometric information is inevitable for the successful application of biometrics to the purpose of combating look-alike fraud. As a consequence, the necessity of decentralised on-chip registration must be reconsidered.
   This last question is a political as well as a social question that can only be adequately answered by taking the forgoing into account.

7 REFERENCES

1. R.H.L.M. van Boxtel, Minister for Urban Policy and Integration of Ethnic Minorities, *Biometrics in travel-documents and electronic identity card*, letter to the Permanent Committee for the Interior and Kingdom Relations of the Second Chamber of the States General, 11 May 2001, BPR2001/U63281 (in Dutch).
2. Robert van Kralingen, Corien Prins and Jan Grijpink, *Het lichaam als sleutel – Juridische beschouwingen over biometrie* (The body as a key – Legal considerations on biometrics), Samsom BedrijfsInformatie bv, Alphen aan den Rijn/Diegem, The Netherlands (1997), ISBN 90 14 05569 2 (in Dutch).
3. Peter Mom, Veel bedenkingen tegen gepersonaliseerde biometrie (Many objections against personalised biometrics), Overheid Innovatief, 2e jaargang, nr. 3, p. 18 (2001), citing J.H.A.M. Grijpink of the Dutch Ministry of Justice (in Dutch).
4. R. Hes, T.F.M. Hooghiemstra and J.J. Borking, *At face value – on biometrical identification and privacy, Report 15 in the series "Achtergrondstudies en Verkenningen" ("Background studies and Investigations")*, Registratiekamer, The Hague, September 1999, ISBN 90 74087 17 5.
5. Samir Nanavati, Real world accuracy: a necessary condition of revenu generation, Biometrics 2001, November 29, 2001.
6. Julian Ashbourn, *Biometrics – Advanced identity verification – the complete guide*, Springer Verlag, London (2000), ISBN 1-85233-243-3.
7. Julian Ashbourn, *User psychology and biometric systems* (1999), http://homepage.ntlworld.com/avanti/.
8. R.L. van Renesse, *Quick scan biometrie – alle mensen zijn ongelijk* (Quick scan biometrics – all people are unequal), TNO report EIB-RPT-990069 to the Ministry of the Interior and Kingdom Relations, 29 October 1999 (in Dutch).
9. Biometric Technology Today, *Fingerprint competition scares off suppliers*, volume 8, number 6, October 2000.
10. Tony Mansfield, Gavin Kelly, David Chandler and Jan Kane, Biometric Product Testing – Final Report, Issue 1.0, 19 March 2001, Centre for Mathematics and Scientific Computing, National Physics Laboratory, Teddington, Middlesex, UK.
11. J.H.A.M. Grijpink (principal advisor for information strategy development at the Dutch Ministry of Justice), Identiteit als kernvraagstuk in een informatiesamenleving: een pleidooi voor een ketenbenadering, (Identity as a basic problem in an information community: a plea for a chain approach), *Handboek Fraudepreventie*, November 1999, Chapter: Fraude en Integriteit – E4010, Samsom, Alphen a/d Rijn (in Dutch).
12. J.H.A.M. Grijpink, Biometrics and privacy, *Computer Law and Security Reports*, March/April 2001, Elsevier Science Ltd., Oxford, UK.
13. Report of the general consultation of the Permanent Committee for the Interior and Kingdom Relations on 21 June 2001, with the Minister for Urban Policy and Integration of Ethnic Minorities, Van Boxtel, on his letter of May 11 2001 [1] (in Dutch).
14. Wendy Atkins, Survey: Banking on finance, *Biometric technology Today*, November/December 2000, Volume 8, no. 7, p. 8-10.
15. *Common Criteria, version 2.1*, ISO/IEC 15408 (1999), addresses the requirements of security functions of IT-products (functionality) and the assessment of confidence levels of security functions (assurance).