Feasibility Study on the Use of Biometrics in an Entitlement Scheme

For
UKPS, DVLA and the Home Office

By
Tony Mansfield,
National Physical Laboratory
and
Marek Rejman-Greene,
BTexact Technologies

Version: **3**
Issued: **February 2003**

Centre for Mathematics and Scientific Computing
National Physical Laboratory
Queens Road
Teddington
Middlesex
TW11 0LW

Tel 020 8943 7029
Fax 020 8977 7091

National Physical Laboratory

Queens Road, Teddington, Middlesex, TW11 0LW

EXECUTIVE SUMMARY

1. This report examines the feasibility of using biometrics as a means of establishing a unique identity, to support the proposed entitlement scheme under development by the United Kingdom Passport Service (UKPS) and Driver and Vehicle Licensing Agency (DVLA).

2. Biometrics identification systems measure physiological and behavioural characteristics of a person, and use these measurements to reliably distinguish one person from another. The main examples considered in this study are fingerprint, iris and face image recognition. Biometric identification can assist in the issue of entitlement cards, passports, driving licences and other identity documents in two ways. On the initial issue of such documents, biometrics can be used to check that applicants are not erroneously issued documents using two different identity details; this is the main focus of this study. Secondly, when an entitlement card, passport or driving licence is being used, biometrics can help confirm that it is being used by the correct person.

3. The purpose of the study is to assess the feasibility of fingerprint, iris and face recognition technologies for these applications, to identify unknowns and the risks associated with the use of biometrics in such a national identity scheme, and to make recommendations for how some of these risks might be addressed should such a scheme proceed.

4. Biometric methods do not offer 100% certainty of authentication of individuals. The success of any deployment of a system using biometric methods depends, therefore, on many factors such as: the degree of the 'uniqueness' of the biometric measure, technical and social factors, user interfaces, and provision of secure back-up systems for those situations and individuals where the biometric will not work effectively.

5. The main findings of the study are:

   a. In principle, fingerprint or iris recognition can provide the identification performance required for unique identification over the entire UK adult population. In the case of fingerprint recognition, the system would require the enrolment of at least four fingers, whereas for iris recognition both irises should be registered. However, the practicalities of deploying either iris or fingerprint recognition in such a scheme are far from straightforward.

   b. Such a system would be a groundbreaking deployment for this kind of biometric application. Not only would it be one of the largest deployments to date, but aspects of its performance would be far more demanding than those of similarly sized systems; such existing systems are either not applied in the civil sector, or operate in countries where public acceptability issues are less prominent.

   c. Current biometric systems are not designed for civil application on the scale envisaged in the UK entitlement scheme. Further work by the biometrics industry is needed to specify how best to use either of the two technologies, and to develop more suitable biometric image capture devices.

   d. The implementation by 2007 of a biometric system to limit multiple identity fraud appears to be feasible, provided necessary background work commences in early 2003. An earlier implementation date does not appear to be achievable.

   e. The use of biometrics will add to the cost of an entitlement card system. The most significant component of this cost is the time and effort to enrol individuals and collect biometric data. However, this is one of the least well-understood aspects of biometric technologies. For example the types and distribution of exceptional cases

will have an impact on throughput performance and choice of an appropriate back-up strategy.

6. We believe that the choice of whether to use fingerprint, iris recognition, or no biometric should be made once additional information becomes available, such as the response from the entitlement card public consultation on the use of these biometrics; and the outcome of further studies suggested in this report that will give clearer information on some of the practicalities of such a large-scale biometric deployment. Ultimately the choice may be based on total system costs.

CONTENTS

1 INTRODUCTION

1.1 About this study

7. This report examines the feasibility of using biometrics as a means of establishing a unique identity, in support of a proposed entitlement scheme under development by the United Kingdom Passport Service (UKPS) and Driver and Vehicle Licensing Agency (DVLA).

8. Biometric identification systems measure physiological and behavioural characteristics of a person, and use these measurements to reliably distinguish one person from another. The main examples considered in this study are fingerprint, iris and face image recognition. Biometric identification can assist in the issue of entitlement cards, passports, driving licences and other identity documents in two ways. On the initial issue of such documents, biometrics can be used to check that applicants are not erroneously issued documents based upon two different identities. Secondly, when an entitlement card, passport or driving licence is in use, biometrics can help confirm that the correct person is associated with the paper credentials.

9. The purpose of the study is to assess the feasibility of fingerprint, iris and face recognition technologies for these applications, to identify unknowns and the risks associated with the use of biometric in such a national identity scheme, and to make recommendations on how some of these risks might be mitigated should such a scheme proceed.

10. Biometric methods can never guarantee 100% certainty of authenticating individuals and systems making use of these technologies need to take this into account. In addition, the socio-technical nature of these systems results in design challenges that have yet to be completely solved – at least for large-scale deployments. Furthermore, for national identity schemes, use of biometrics may not address all of the requirements. Indeed, there may be no single, cost- effective solution that meets all of the expectations that government, the criminal justice system, commerce and the citizen place in these schemes [1].

1.2 Size and timescales

11. It is proposed that the scheme applies only to people over the age of 16. This results in a coverage of approximately 50 million people, although a provision for removal from the scheme on death may need to be implemented.

12. The original suggestion was for the scheme to be implemented by 2005, and over the following 10 years for all over 16s to be entered into the system. It is unlikely that the throughput would be uniform over this period, as the scheme would be used for passports, driving licences as well as entitlement cards, each with their specific issues and renewal cycles. We have assumed that the daily throughput could range between 10,000 and 50,000 enrolments.

13. Once the scheme has been rolled out across the adult population, the system will only need to deal with rising 16 year-olds and new foreign residents, requiring a daily throughput of approximately 3000 enrolments.

14. The UKPS/DVLA proposals assume that applications are processed, and biometric images collected at local offices, in a manner similar to the current process of checking and driving licence applications by the High Street partners of UKPS and DVLA. We assume a similar number of local offices (i.e. approximately 2000).

1.3 Use of biometrics to authenticate identity

15. Biometric methods of authenticating the identity of people make use of physical characteristics or actions that are sufficiently individually defined to meet the requirements of a specific application. The key to successful use of these methods depends on a number of factors:

a The extent to which the system operates without human intervention;

b The degree of 'uniqueness' of that feature and any resulting confusion with other identities in the group;

c Technical factors such as security, robustness, cost and scalability;

d Social factors such as acceptability and trust in the operators of the system.

16. Perhaps the most obvious biometric method uses *fingerprints*, building upon the century of experience in the detection and prosecution of criminals. Recently, automated fingerprint identification systems (AFIS) have been developed to search the database of prints so as to identify a person against a latent print found at a scene of crime. This is a *one-to-many* search. The other way of using this biometric is in verifying a person's claimed identity, by a *one-to-one* match, comparing the fingerprints of a person with a specific set obtained on an earlier time when the identity was established with reference to documents, etc.

17. Numerous biometric characteristics and actions have been proposed and some have been developed to the point where they are available commercially. Automatic *facial recognition* systems derive from the ability of humans to distinguish individuals by relative proportions of facial features, although—as in the case of human recognition—the discrimination is relatively limited. Nevertheless, the widespread use of photographs in identity documents and the familiarity and general acceptance by the public at large ensure that this technique will be used in some form in national identity applications.

18. Much better performance in identification is possible by using features in the eye. The original approach made use of the pattern of fine blood vessels in the retina at the rear of the eye. Special binoculars were developed to image these retinal features, and although the ability to discriminate between individuals was very good, it proved difficult to use by the majority of the public. In contrast, *iris recognition* cameras photograph the coloured part of the eye and are easier to use, less intrusive and still provide a very good level of discrimination.

19. Biometric systems work by converting the captured image into a *template*, a more compact version of the image that captures just those features of the image that contribute to the distinctiveness of each person's eye or fingerprint, etc. When a person needs to have their identity verified, another image is taken and processed into a form that allows comparison with the template. In general, people will never present themselves in exactly the same way, and biometric systems will always have to allow some latitude in this matching process for the system to work. However, with too much latitude a person might match templates other than their own. The trade-off between people failing to match their own template (*False Non-match Rate*) and matching those of others (*False Match Rate*) can often be tuned to make the system easier to use or more secure depending on the application. Of course, some people will find difficulty in using the system and the *Failure to Acquire* rate is a key factor in determining whether a biometric method can be used. In any case, some form of back-up strategy needs to be developed.

20. In addition to fingerprint, face and iris recognition, there are systems based on individuality in written *signatures* and *voice* characteristics. There are also *hand geometry* biometric systems that make use of distinctive shapes of the hand and fingers. These are less accurate and less likely to fit with scenarios of use in entitlement card applications. For the purposes of this study, we have considered the merits of iris and fingerprint recognition techniques as the primary methods of checking for uniqueness of identity; and facial recognition as a way of resolving residual ambiguities as well as offering a quick method of verifying identity at a government office.

21. In this study we concentrate on fingerprint, iris and face recognition biometrics.

a. There are around 100 suppliers of fingerprint systems, and several types of sensor and algorithms with varying performance characteristics. However most large-scale implementations deploy technologies from a few leading AFIS suppliers.

b. In the case of iris recognition, almost all systems use the same underlying patented algorithms [2] for comparing iris patterns. The main differences between systems being in the camera systems, user interfaces, and 'liveness' checks.

c. For face recognition there are several suppliers, with most implementations using technology from one of a few suppliers.

For large-scale identification systems, the system integrator is not normally a biometrics supplier, as the biometric component is usually a minor part of the identification system. System integrators may work with several different biometric suppliers.

2 USES OF BIOMETRICS WITHIN THE ENTITLEMENT SCHEME

22. Biometric identification has three potential uses in an entitlement scheme.

a Ensuring a unique identity by checking to prevent duplicate applications;

b Verifying that the person presenting an entitlement card is the person to whom it was issued; and

c Checking the identity on the card against a 'watch-list' of a selection of facial or fingerprint images.

Each of these constitutes a separate application, with different performance requirements; the optimal way to use any biometric will depend on which of these three applications is under discussion. The following sections illustrate possible scenarios for operation of the biometric function in each of the three cases.

2.1 Establishing a unique identity

23. The main application we are concerned with in this report is the use of biometrics to help establish a unique identity when applying for a passport, driving licence, or entitlement card.

2.1.1 Outline procedures

24. The UKPS/DVLA Working Group suggest that enrolment into the identity system would normally take place at local offices, in a similar way to the high-street partners of the UKPS and DVLA that check and assist with passport and driving licence applications.

25. These 'front offices' would:

a Check the application and supporting documentation;

b Capture the identifying biometric (fingerprints or iris images) and take a photograph;

c Electronically submit the biometric details to the identification system for checking identity;

d Electronically submit the application to UKPS, DVLA, as appropriate;

e Handle the remittance.

26. For most people, presenting a biometric of sufficient quality for identification should take a matter of seconds and require no operator assistance other than advice on how to use the system. However, it is recognised that this will not be the case for all people. We envisage that in cases of difficulty, some operator assistance will be needed, and it may be necessary to use a modified system for collecting the biometric. Moreover, it must be accepted that, regardless of the choice of biometric, a small proportion of the population will be unable to enrol. Some people will have missing fingers, eyes or irises due to disease or disability. In such cases identity will need to be checked using the current processes rather than through use of the biometric database. The size of these exception groups will impinge on the feasibility and costs of operating the identity system. Furthermore, some people will be physically unable to attend the front office. In such cases, a remote enrolment unit could be used.

27. The 'back-office' of the identification system would automatically check the biometric details against the existing database. In the case of new applications, this will involve a search of the existing database for any closely matching biometrics. If there is no close match, the application is unlikely to be for a duplicate identity, and the biometric and personal details

will be added to the database. If there is a match, there is a presumption of application for a duplicate identity. Such possible duplicates will need to be confirmed or refuted manually, and to support this process the identity database should store some personal details in addition to the biometric. A photograph is particularly useful in this respect. If the identity remains suspect after such a check, the individual would be called for a face-to-face interview. Clearly the acceptability of the system depends on very few genuine applicants being subjected to this further series of procedures.

28. In cases such as renewal, or application for a second or third type of identity document, the applicant's biometric details should already be held on the database. In such circumstances, the biometric identity check could be used:

a To prevent identity take-over by someone masquerading as the original applicant;

b To check, and correct, personal details (e.g. spelling of names, address details) as required;

c To determine whether the stored biometric should be updated. As people age, their biometric details will gradually change from their enrolled biometric templates. Periodically updating the biometric template can help the system maintain the best possible performance, particularly if the biometric is used for authentication of an entitlement-card holder. In the case of iris or fingerprint, which are relatively stable throughout adult life, updating might only be needed in cases of major trauma to fingers or eyes. However, face recognition systems are likely to require an update at least every 10 years.

2.1.2 Performance requirements and choice of biometric

29. The performance requirements for this identification application are very stringent. The identity database will eventually contain biometrics for over 50 million people, and the yet the probability of a chance match in biometric identities—requiring manual checking—must be very low. Meanwhile capture of the biometric image needs to be quick, require little or no operator assistance, and yet generate biometric images of sufficient quality that the chances of a false non-match that could result in a duplicate enrolment are remote. The stringent performance requirements rule out most biometrics other than fingerprint or iris recognition.

2.1.2.1 Fingerprint recognition

30. In the case of fingerprint, we suggest that flat prints of all fingers should be collected. (Flat prints are preferred to rolled prints due to the speed and ease of collection.) The search of the fingerprint database might be made using, say, four fingerprints with the remaining prints used to help verify any potential false matches (see Section 3.1.1). Face recognition biometrics, based on a photograph taken at the same enrolment session, might be used in the checking process, thereby possibly reducing the number of fingers required. However this possibility does not appear to have been investigated by any biometric supplier, and our considered opinion is that it would still be necessary to use at least four fingerprints.

31. Current large-scale fingerprint applications are minutiae-based, that is they operate using the coordinates of points on the fingerprint where ridges end or split. There are also systems that use the whole of the fingerprint pattern. Pattern-based systems may offer some cost and performance advantages for one-to-one verification, but the minutiae-based approach is preferred for one-to-many matching. Firstly this is the approach used by all current large-scale AFIS systems, and there is little knowledge of scalability of the pattern-based approach. Secondly standards are well advanced for recording minutiae based fingerprint templates; this allows greater interoperability, and choice of suppliers. Thirdly, for large databases, minutiae

comparison is quicker than an image-based comparison, which is a crucial consideration when each enrolment needs to be compared against 50 million existing templates.

Recommendation 1. For the identification application, if a fingerprint system is used, it should be minutiae based.

32. Worldwide, there are several fingerprint systems that are being used to help establish a unique identity per individual. Examples mentioned in this report include:

a. In the UK, the Immigration and Nationality Directorate (IND) fingerprint asylum seekers to determine whether they are already known to the system, and to issue Application Registration Cards (ARC). Approximately 400,000 asylum seekers are enrolled in this system.

b. In the Philippines the Social Security ID System (SSS-ID) [3] uses fingerprints to help prevent instances of multiple SSS number ownership, and issues an SSS card containing the biometric as a two-dimensional barcode. To date some 3 million people are enrolled in the system out of a population of 35 million.

c. Though not a civil system, in the USA, the Integrated Automated Fingerprint Identification System (IAFIS) [4] of the Federal Bureau of Investigation, has fingerprint records for over 40 million individuals and is of a similar scale to that required by the entitlement cards proposal.

2.1.2.2 Iris recognition

33. Iris recognition has attractive performance characteristics; a single iris image provides as much identification evidence as two or more fingerprints. As there will be cases where it is difficult to capture more than a small proportion of an iris, we recommend collection of both iris images. This also allows for situations where one eye is unusable, e.g. due to injury.

34. Iris recognition is a relative new biometric technology, and there are few large-scale applications. One of the largest applications to date is for refugees returning to Afghanistan from Pakistan, where the United Nations High Commissioner for Refugees (UNHCR) is using iris recognition to help stem fraud whereby some refugees were doubling back across the border to claim repatriation allowances multiple times. Over 60,000 people are enrolled in this trial.

2.1.2.3 Face recognition

35. Face recognition on its own is a long way from achieving the accuracy required for identifying one person in 50 million (see Section 3.1.1). Several recent trials of the technology have shown relatively poor identification performance even for quite small populations. A single fingerprint provides higher accuracy than face recognition, and while fingerprint identification can be improved by using multiple fingers, this option is not available for face recognition. A further drawback is that face images are genetically determined, and face recognition cannot reliably distinguish between identical twins (in contrast to fingerprint and iris recognition—approximately one person in a two hundred has an identical twin.

36. Automatic face recognition could, however, be deployed for one-to-one verification of the entitlement cardholder, for small watch-list applications, or possibly as an investigative tool to assist in finding duplicate enrolments.

37. An example of how face recognition can assist in finding duplicate enrolments is the system developed for the 2000 presidential elections in Mexico. Here face recognition is used to help detect duplicate voter registration when name and other details seem suspiciously similar.

2.1.2.4 Combining biometrics

38. It is, of course, possible to use a system with both fingerprint and iris biometrics. This can improve performance, and would reduce the number of exception cases where people are unable to produce the required biometric, as there are very few people with neither irises nor fingers. Use of multiple biometrics in this way also allows greater possibility for interoperability between systems, and retains the option of upgrade to future systems. However the performance improvement is unlikely to be commensurate with the increased costs, and collection of the additional biometric images might be seen as unnecessarily intrusive by the public.

2.1.3 Identity database

39. It is envisaged that the identity database would contain:

a. Personal details including name, date of birth, sex, and possibly address. This data helps to correctly resolve cases of matching biometrics while minimizing the number of cases where the applicant must be called for interview. It is also needed in cases where the applicant cannot provide the biometrics being used by the system.

b. Biometric details: i.e. fingerprint *or* iris templates.

c. Photograph, and possibly face recognition biometric template based on the photograph. (Automatic face recognition often uses a digitised face image as a template.)

d. Cross references to issued identity documents, passport number, driver number, etc.

e. Date/office/enroller for the biometric enrolment; this information can be used to audit the system for security.

40. Additionally we recommend that the raw images should be kept in a separate back-up database. This database does not need to be automatically searchable. It would be used in case of change in supplier, upgrades of algorithm etc that warrant a new template format. Otherwise re-enrolment of the population already registered would be required. The database could also be used to help resolve false matches, and, if appropriate, support prosecution in the cases of identity fraud.

Recommendation 2. Store raw biometric images to allow for future algorithm changes. These images do not need to be stored with the identity database for fast retrieval.

41. There are other options for the database that avoid linking personal details to the biometric data of subjects. For example the database could contain only the biometric templates, allowing the possibility of checking for potential duplicate enrolments. Such a database would not provide information on the matching person to help resolve whether the match is evidence of a true duplicate. Selecting this anonymised database option would require higher performance and accuracy, together with alternative checking procedures.

Recommendation 3. Investigate the options for alternative, privacy-enhancing, database architectures that may offer a measure of security against duplicate issue of identity documents and responds to criticisms of comprehensive national registers.

2.2 Verification of card-holder

42. Verifying the identity of an entitlement-card holder is a simpler application. The entitlement card, passport or driving licence may be issued containing a biometric template in the form of a two-dimensional barcode, or in the integrated circuit on a smart card. The ‘on-card’

biometric templates need not to be the same as those used to establish a unique identity held in a central database.

43. When the cardholder is required to verify their identity, they would place their smart card into a combined biometric/smart-card reader, and present their biometric to the system. In this instance, the remote biometric system need only compare the presented biometric against the templates stored on card—without reference to the central database. As it is in the cardholder's interest to present their biometric in a way that maximises the likelihood of successful identification, this simplifies task for a biometric system, and fingerprint, iris or face recognition could all be feasible technologies.

44. Though the required performance levels would typically be achieved by a single fingerprint or single iris, we would recommend storing two fingerprint templates or iris templates on the card as this allows some robustness against problems or difficulties with a particular finger or eye.

45. How false rejections should be handled will depend on the particular application and the reasons for cardholder verification: additional checks may be possible, for example using the photograph and other details stored or printed on the card, or it may be possible to call-up the central identity database for confirmation.

46. Use of a biometric along with the card provides two-factor authentication. This could be made yet more secure against false acceptances by also requiring a PIN or password.

2.3 Watch-list

47. A further potential application for biometrics, applicable in the case of passports, is for use in matching people against a 'watch-list'.

48. A watch-list of face images or fingerprint records might be maintained, where it is desired to know whether these people are travelling. At a checkpoint, a fingerprint or face biometric on the passport/card can be read and compared against the images on the watch-list. The system can then indicate the most likely matches to an operator, simplifying their task of checking passengers for those on the watch-list.

49. Both face and fingerprint biometrics are suitable for this task. In the case of face recognition the watch-list must be relatively small in size, but for fingerprint can be much larger. Indeed the fingerprints stored on US Immigration and Naturalization Service (INS) Border Crossing Cards are routinely checked against a large database of criminal aliens.

3 PERFORMANCE ISSUES

3.1 Identification accuracy

50. The accuracy of identification of biometric systems depends on a number of basic performance measures:

a The *false match rate* measures the probability that a person's biometric matches the enrolment template of another person.

b The *false non-match rate* measures the probability that a person's biometric fails to match their own enrolment template.

A biometric implementation can trade-off these two error rates by setting a threshold that determines the degree of similarity required between the captured biometric and stored template before the similarity is deemed a match. A stricter setting for this threshold will decrease the false match rate at the expense of increasing the false non-match rate and *vice versa* for a more lenient setting.

c The *failure to acquire rate* measures the probability that the submitted image is of too poor a quality for the system to make a reliable decision on identity. Often systems will treat a failure to acquire as a non-match decision, and the failure to acquire rate becomes part of the false non-match rate. However, this is inappropriate when checking that a person is not already enrolled. In this circumstance, by presenting a poor quality biometric a person could trigger a non-match and thereby obtain a duplicate entitlement card.

51. There have been a number of recent studies into biometric system performance [5-8] that provide a starting point for estimating the approximate performance of fingerprint, iris or face recognition biometric systems when applied in different aspects of the entitlement card system. It is important to note that performance figures depend critically on the specific application, the demographics of the population, and the operational environment. Pilot implementations will be necessary to obtain good estimates of performance in the deployed applications, and are an obligatory part of the tendering and implementation processes. The figures given here are indicative of achievable performance, using leading biometric technologies, in a good implementation, and ensuring good conditions for data collection etc.

52. The performance studies indicate that, for the respective technologies:

a For a single matching attempt against a single finger, some good fingerprint systems are able to achieve a false match rate of 1 in 100,000 with a false non-match rate of approximately 1 in 100. (Results based on Fingerprint Verfication Competitions FVC2000 [7] and FVC2002 [8].) However, this level of performance will not be sustained if the fingerprint images collected are of poor quality.

b Iris recognition can achieve a false match rate of better than 1 in 1,000,000 with a false non-match rate of below 1 in 100, provided the system classifies incorrect presentation as an acquisition failure (Results based on an evaluation for the UK Government Biometrics Working Group (BWG) [6], and an evaluaton using a large database by the principal technology supplier [9]).

c In the BWG evaluation [6], face recognition achieved a false match rate of 1 in 1000 with a false non-match rate of 1 in 10. This level of performance was realised under ideal lighting conditions and with subjects directly facing the camera, and with test

images taken 1 to 2 months after enrolment. In the Facial Recognition Vendor Test FRVT2000 [5, Test T3], with a longer timespan between enrolment and verification attempts, and with less ideal illumination, performance is degraded somewhat (a false match rate of 1 in 1000 would result in a 6 in 10 false non-match rate!). Even under relatively good conditions, face recognition fails to approach the required performance.

53. It is possible to reduce false match rates by using two or more fingers in the case of fingerprint systems, or both eyes with iris recognition systems. Similarly, for verification applications, allowing more than one attempt can reduce the false non-match rate.

Recommendation 4. Pilot implementations as part of the tendering and implementation process will be necessary to obtain good estimates of performance in the deployed applications.

3.1.1 Accuracy of a 'one-to-many' identity search

54. In the case of a database search to determine whether an individual already has been enrolled we are concerned with two types of error:

a False alarms, where an unenrolled person is falsely matched against one of the existing biometric templates, thereby denying that person their entitlement card, passport or driving licence; and

b False non-matches, where an enrolled person does not match their enrolment template thereby allowing an application for a second entitlement card, passport or driving licence.

55. As the person's biometric is compared against every template in the database, the false alarm rate is very dependent on the number of people in the database. As the numbers of subjects in the database increases, the probability of a false alarm increases correspondingly The false alarm rate depends on the number N of people in the database according to the formula

$$\text{FalseAlarmRate}(N) = 1 - (1 - \text{FalseMatchRate})^N$$

In our case the database size will eventually be approximately 50 million, and yet the false alarm rate must remain very low as each case will require manual (and expensive) checking. With a daily throughput of several thousand applications, a target of less than 1 in 1000 for the false alarm rate offers a reasonable compromise, while a false alarm rate of much above 1% would probably make the system unworkable. This implies that the false match rate for every single comparison must be at most 1 in 10^{10}, and preferably, 1 in 10^{11} or better. With the known performance of fingerprint, iris and face biometric systems, this requirement mandates the use of multiple fingers, or irises, and confirms that facial recognition is not a feasible option.

56. A second requirement is for a low probability of missing a duplicate enrolment. Here the requirements are less stringent. A 90-95% chance of detecting a second enrolment is probably sufficient. This appears to be achievable even when both irises, or several fingers, are mandated. One proviso on the acceptability of this 5-10% false non-match rate is that the false non-matches are evenly spread over the population; clearly, it would be unacceptable for some individuals to consistently not match to their enrolment templates, as such users might be tempted to obtain a second identity without running the risk of detection.

57. For a fingerprint identification search in a database of 50 million people, fingerprint system suppliers, and other organisations (e.g. the Mitretek study for NIST [10]) have investigated how many fingerprints are required. Results show that at least four fingers should be used in

such a system, and that it is beneficial to collect prints of the all fingers to to reduce the incidence of false alarms even further.

Recommendation 5. For fingerprint recognition to uniquely identify one person in a population of 50 million at least four fingers per person are needed. Collecting prints from all fingers is recommended.

Recommendation 6. For iris recognition to uniquely identify one person in a population of 50 million we recommend using images of both irises.

Recommendation 7. Face recognition is not strong enough to uniquely identify one person in a population of 50 million.

3.1.2 Accuracy of 'one-to-one' identity verification

58. For one-to-one identity verification, it is only necessary to use a single finger, a single iris, or face recognition. The matching error rates achievable are those previously mentioned in Section 3.1. Performance can be further improved if multiple attempts are allowed, though this will make the systems slower to use.

59. For verification, the performance of a single finger, single iris, or face biometric is likely to be sufficient for most applications. Nevertheless we would suggest that, in the case of fingerprints, the entitlement card or identity document carries templates for two (index) fingers in case one is unavailable (bandaged). Similarly, if iris recognition is used, template for both irises may be used for verification.

Recommendation 8. Identity verification should use an on-card template on card, not accessing templates from the central (identification) database.

3.1.3 Watch-list performance

60. We start by assuming that the watch-list system works by alerting an operator if it detects a person sufficiently similar to someone on the watch-list. In this case the error rates of interest are the rate of false positives (or false alarms), i.e. the probability that the operator is alerted when the person is not on the watch-list, and the rate of false negatives, i.e. the probability that someone on the watch-list does not cause an alert. Formula for these error rates are:

$$\text{FalseAlarmRate} = 1 - (1 - \text{FalseMatchRate})^{\text{Watch-listSize}}$$

$$\text{FalseNegativeRate} = \text{FalseNonmatchRate}$$

As face recognition cannot achieve a false match rate of much better than 1 in 1000 without an unacceptably high false non-match rate, these formulae imply that face recognition technology is not suitable for applications with a watch-list of size much over 1000.

61. We note that the watch-list application will compare the biometric stored on the entitlement card or identity document against watch-list images collected by other applications. Performance will be best if the images used for both the identity document biometric and the watch-list are taken in similar environments controlled for near optimal performance. With poor quality watch-list images (or poor quality biometric enrolments) performance will deteriorate considerably. In fact, there may be little value in having poor quality images on the watch-list.

62. A second point to note is that recent trials of face recognition for watch-list applications at airports compare live face images against the watch-list. It is hard to collect good quality face images of all people passing a fixed camera as, for example, some people will not look in the right direction. Thus comparing the face biometrics on an identity document against the

watch-list ought to give better performance than these recent trials, again provided that the enrolled face images are of good quality.

63. A second way to use a watch-list is to return for each person the top matching images on the watch-list, with the operator checking the person against these images. This method is more suited to situations where an operator is already performing such checks unassisted, as the biometric assistance will improve their performance

Recommendation 9. Performance of face recognition is satisfactory for watch-lists of size up to approximately 1000. (With this size watch-list, and with good quality enrolments and watch-list images, 50%-90% of people on the watch-list will be correctly matched to their watch-list image.)

Recommendation 10. If face recognition biometrics are to be used, the face photograph should be taken at the 'front office' where it can taken in accordance with appropriate standards [11] to ensure best possible performance.

3.2 Analysis of failure to acquire rates

64. At initial enrolment, there will be times when the image presented by the user and obtained by the system is not of sufficient quality to properly process as a biometric. If such images are used, failure to match the correct (or indeed any) template would be guaranteed. Many existing biometric systems do not apply strict quality controls, as they are not normally operating in negative-identification mode (where a failure to match means that an entitlement is allowed).

65. In the case of acquisition failures, the appropriate action to take depends on the equipment being used, any secondary equipment available, and the reason for the failure to acquire.

a Clearly the set-up around the enrolment station at the front office should eliminate any environmental causes of failures to enrol. For example, in the case of iris recognition any stray illumination sources causing the iris camera to see reflections on the eye should be eliminated.

b Sometimes a second attempt at presenting the biometric, with some additional advice from the operator will achieve a good quality image. For example, in the case of fingerprint recognition, a failure to acquire may be due to damp, dirty or dry fingers, which can be remedied by the user washing his or her hands, or by applying hand cream in the case of dry fingers.

c In other cases there may be fundamental reasons making it difficult or impossible to present the biometric in the normal way. For example in the case of iris recognition, people that are blind or blind in one eye would find it almost impossible to correctly position their eye if they need to look at that eye in a mirror. For such cases an operator hand-held iris camera may be useful. In the case of fingerprint recognition, users with arthritis will find it difficult to present flat prints on a standard capture device, and they may need to be enrolled one finger at a time on a different device.

d Sometimes people might not have the biometric being used. In the case of iris recognition for example, the inherited condition 'aniridia' means that approximately 1 in 70,000 of the population are born without an iris. Taken with other relatively rare conditions such as iris coloboma, anophthalmia, etc. perhaps 1 in 10,000 people do not have an iris that can be used for iris recognition. In the case of fingerprint recognition over 1 in 1000 fingers are missing, or have no fingerprint but only scar

tissue. In such cases no biometric can be collected, but other identity checks can be made to allow the person their passport, driving licence or entitlement card.

e A further category of people that are not enrollable consists of those unable to access the front office, for example people who are housebound. Portable devices might be used to enrol such people. Examples are already in use for fingerprint systems, e.g. by IND, and have been developed for iris recognition.

66. The exact sizes of the exception groups are unknown, and will depend considerably on the extent of human assistance available, the ease of use, and the clarity of operation in the implemented system. In the case of fingerprint systems it has been observed that women, children, older people, and those involved in manual work tend to have worse quality fingerprints, and are perhaps more likely to fail to give good quality fingerprints at the first attempt. Face recognition is the most universal of the biometrics, but even so there will be times when automatic enrolment fails, and the template construction must be completed with human assistance in identifying feature points on the face image.

Recommendation 11. For identification, the biometric component must treat failure-to-acquire errors separately from failure to match by system.

Recommendation 12. In addition to the normal equipment and processes for biometric image capture, versions will be needed to provide additional assistance in problem cases, and for collection of the required biometrics away from the front office.

Recommendation 13. A study is required on the size and types of failure to acquire population, in order to decide the appropriate secondary methods for biometric image capture for exception cases.

67. For such a study to show a statistically meaningful sample of exception cases, a pilot implementation needs over 10,000 individuals representing all sections of the population. A subset of this group could be specifically selected to examine previously documented problem populations in more detail (e.g. for fingerprint systems, those engaged in manual work, persons of East Asian origin and pensioners).

68. A study on exception cases of all types should be included as part of the design process for the entitlement scheme, specifying the data to be collected during the initial rollout as part of a process to alert the deployment agency of unexpected problems.

3.3 Throughput rates

69. An important consideration for the successful deployment of the entitlement scheme is the speed with which users can enrol onto the biometric system. This will consist of a number of elements:

a Time required for presentation of the operation of the system by the attending official and for the reading of any information from the terminal screen;

b Initial demonstration of the process for obtaining a biometric image;

c Capture of the biometric image;

d Response by the system after quality checks;

e Possible remedial action if quality checks fail, (e.g. cleaning the hands in the case of fingerprints);

f Confirmation of correct operation of the biometric and demonstration of the performance to the subject, through a verification process;

g Further opportunities for discussion between the subject and the attending official;

h Re-enrolment in instances of process failure.

70. The total time for enrolment is often considerably longer than anticipated from addition of the individual times for each of the elements. Experience from testing of biometric solutions at the [6], with technically aware users and a very simple biometric, gave average times for enrolment of approximately 5 minutes per system. Obviously, exceptional cases will take considerably longer, and the 'exception' study of Recommendation 13, above, should include a consideration of the impact on throughput rates.

71. Another example is the Privium system at Schiphol airport where enrolment takes approximately 20 minutes per person. Approximately 5 minutes of this time is spent enrolling iris images in the system, the remaining time being spent in checking the application form, a background checks against the police database, and training attempts at an example verification.

72. We assess the core capture time for fingerprints. Collection of multiple fingerprints is likely to be quickest in 'slap' mode, using a large-area biometric-platen able to image all fingers on one hand in one scan. The capture process might then involve just three 'slaps' (fingers on right hand, fingers on left hand, then thumbs). This process might take approximately 20 seconds to capture all 10 fingerprints, provided there were no problems of poor quality fingerprints requiring remedial action or a second fingerprint capture. If fingerprint images are collected one at a time, the process will take somewhat longer, moreover additional care is required to ensure that the fingerprint images are taken in the correct order (in fact 'slaps' are often collected to ensure that individual prints taken are assigned to the correct finger). Collection of 'rolled' prints is still slower (3 to 5 minutes) and requires direct operator assistance to roll each finger separately. This is likely to be considered more intrusive by the public. Rolled prints are preferred in the criminal justice system as this provides more forensic information per finger, for matching against latent prints etc. Inked prints are a possibility for capturing fingerprint images remotely, but from discussion with fingerprint vendors, and staff working on the UK IND asylum seekers fingerprint system, these are prone to image quality problems.

73. In the case of iris recognition, current systems capture images of each eye separately. For each eye, users must align themselves carefully, and the camera needs time to auto-focus on the iris. At enrolment the system also applies strict quality checks on both focus and the amount of the iris visible between the eyelids, often causing a further attempt at enrolment to be required. We believe there is scope for improving the iris image-capture process, making it faster for users not familiar with the technology. The newest iris recognition camera (the Panasonic BM-ET500) does not appear to require as precise positioning as the current cameras, and this may speed up the enrolment process.

74. Additional time will be required for users to get into position, for instruction on how to present their fingerprints and on how the system operates, and for the remedial action and additional attempts that will be required in many cases.

75. A separate consideration is the off-line identification of individuals where the throughput rate will be determined by considerations of algorithm efficiency, optimised design of databases, specialised hardware, etc. Once the majority of people are enrolled into the system, any application involves a check of the applicant's biometric against approximately 50 million others, and there may be 10 to 50 thousand such checks per day. Such a biometric search is highly parallelisable, and with both fingerprint and iris recognition systems the required throughput is achievable by increasing the number of processing component in proportion to

database size. (The occurrence of errors requiring human resolution must, however, be sufficiently rare that errors can still be handled when the system has scaled to maximum throughput. This necessitates the very low false match error rate discussed in Section 3.1.1.)

Recommendation 14. If the identity system uses fingerprints, collect flat prints rather than rolled prints. Furthermore, make use of 'live-scan' electronic capture fingerprint devices in preference to the digital scanning of inked fingerprint cards.

4 SECURITY ISSUES

76. The biometric sub-system is part of a full IT system implementing the entitlement scheme. The system security policy should therefore reflect the specific issues associated with the use of these novel authentication technologies, in particular addressing the issues associated with probabilistic identification, handling of exception cases and resort to the use of back-up alternatives. Human and social vulnerabilities and security threats should be identified and technical and procedural measures implemented that limit the opportunities for internal and external compromise. To support this aim, a number of existing and emerging standards for biometric security should be considered, e.g. ISO 17799 [12] and ANSI X9.84 [13].

77. ANSI X9.84 "Biometric Information Management and Security" lists several security considerations and possible attacks or weaknesses in biometric systems. This list includes:

a Registration of an individual using a false identity;

b Fraud susceptibility within data collection using a synthetic fingerprint, iris or face image;

c Vulnerability of data during collection, transmission and storage on the central database;

d Injection of false biometric, replayed biometric, or identification decision into the system;

e An attacker searching the database to identify individuals with similar biometric features;

f Improper threshold settings, device calibration, illicit device, flaws in system performance;

g Compromise of biometric data affecting privacy.

78. The second of these security considerations (77.b) is specific to the use of biometrics.

a How easy is it to fake the biometric, in order to be incorrectly verified as an entitlement-card holder? That this is possible is evidenced by the addition of 'liveness' testing features to some biometric systems. Depending on the sophistication of these countermeasures, the systems can be made more or less difficult to spoof. Biometric suppliers must continue to work to improve countermeasures in order to stay ahead of attackers.

b How easy is it to disguise or modify one's own biometric in order not to match against your existing identity in the database? If enrolments are closely supervised, the use of fake biometrics will generally be easy to spot, though the operators need enough detail about potential attacks to know what to look for. Some ways of altering the biometric to avoid recognition should be treated as failure to acquire. For example user of eyedrops to dilate the iris will prevent recognition, but the effect is detectable by the system, and the enrolment quality control system should deemed the iris image invalid.

79. Iris recognition is generally more resistant against fakes and modification of the biometric than fingerprint systems. This is partly because people are unwilling to damage or alter their eyes to make a spoof attempt, but also due to the countermeasures employed. The more sophisticated iris imaging systems are resistant to the use of photographic images and printed

contact lenses for example. In contrast, a recent study [14] showed that currently many commercial fingerprint systems can be spoofed using artificial gelatine fingertips.

80. To date, only two systems have been evaluated (or are being evaluated) under the Common Criteria scheme for information technology security evaluation. One is a fingerprint application, the other an iris recognition application. Such evaluations are relatively expensive for the small biometric companies involved, and evaluations to high Evaluation Assurance Levels are unlikely unless sponsored by the client of the biometric system, or made a requirement for procurement. This will become easier once work concludes on developing Common Criteria Biometric Protection Profiles and Biometric Evaluation Methodology. Such evaluations will always require the supplier to be sufficiently open about their design and implementation in order that the security can be independently assessed.

81. Security must also address user privacy issues, and possibilities for collusion between the staff operating the system and members of the public. In particular, the biometric image and templates should be encrypted, dated, timed and digitally signed for any transmission to protect against replay attacks. In this respect, for one-to-one cardholder verification, it can be best if the templates are held on card, as then there is no need to transmit biometric details to/from a central database.

82. A further aspect of concern is that an insider may mount an attack by using the database to search for matches between pairs of biometric templates. The system itself does this to prevent duplicate identities but, if the results are not kept secure, the attacker may collude with the owner of one matching template to defraud the owner of the other template.

Recommendation 15. The security of the identity database is very important. The database must be secure against fraud, and not introduce possibilities for further fraud. A security evaluation of the system must be carried out.

5 PROCEDURES

83. Procedures and processes will be determined to a large extent by the specific details of the implementation of a biometric-enabled application together with the need to interface with existing processes and organisational cultures at the UKPS, DVLA and the agency responsible for the national biometrics database. Nevertheless there are general considerations that will apply to most systems.

5.1 Procedures at 'front office'

84. The most critical, and expensive, aspect of the entitlement card scheme will be the enrolment office and the procedures that ensure fast resolution of problems. If users understand the biometric method and what is expected of them, the contact time with the enrolment officials will be reduced, and the probability of obtaining a high quality template will be improved. Priming through education in the period immediately prior to attendance at an enrolment centre will be critical and a well-designed user experience at the centre is a pre-requisite for success. Current biometric devices will require extensive redevelopment, and the government agency will look to the system integrator to refine the rather unfriendly interfaces and operational procedures. Customised units should reassure and invite the user to co-operate with the enrolment process..

85. Training of enrolment officials need not be a major undertaking, as evidenced from the IND experience, where agency staff are used. However, procedures for a sensitive approach to exceptional cases will be required, whether this is for people with absent features, poor quality features or when a possible duplicate enrolment is flagged. A backup strategy for those people who are unable to enrol will need to be developed and validated, with clear guidelines that limit the possibility of abuse. Anti-collusion procedures are also required, with separation of critical duties employed wherever possible and the signing of an enrolment instance in the database with the electronic signature of the enrolling official.

86. We believe that simple flat finger systems are far preferable to the traditional 'rolled' fingerprints of police systems. Although there is a reduction in the number of minutiae that can be used in a template, the faster throughput and distinction from police procedures should outweigh the loss of information.

87. The experience gained in many trials over the past decade should be used in enrolment procedures. For example, a warm environment will increase the probability of obtaining a better image and access to cleansing materials should be specified to ensure the best possible enrolment.

88. If an iris recognition system is specified, a procedure that limits the source of unwanted reflections should be developed. Removal of spectacles and designer contact lenses is clearly desirable. A high level of illumination will ensure that the pupil size is minimised with a resulting increase in the size of the visible area of the iris. Note that drooping eyelids may cover some of the iris area and currently offered systems may reject such subjects, therefore some people may be required to hold their eyelids apart.

89. Little is known about long-term performance of biometric units and the Service Level Agreement should define uptimes and quality procedures to ensure continued operation at the agreed performance specification.

90. Even though some biometric techniques (as distinct from specific devices) have been evaluated over a period of 30 years and more, there are very few studies that have tracked

individuals over a significant part of a person's life. The implications of *template ageing* are still to be determined. Fingerprints and iris patterns templates should be considerably more stable than facial images, although the relative performance of the algorithms used by competing suppliers of face recognition systems remains unclear. The general pattern in most biometric methods is for a rapid change over the first few weeks, followed by a gradual drift and consequent loss of performance on verification thereafter. Young people will be expected to change faster, but there is little reliable data. Therefore, to maintain optimal performance, there may be a need for periodic updating of the biometric templates.

a In the case of face recognition it would seem advisable to update templates at least every 10 years, and more frequent updating may be required.

b Fingerprints are relatively stable throughout adult life, but if children (below 16) are included in the scheme, it may be necessary to update their fingerprint templates once they are fully-grown.

c If the biometric is used for one-to-one identity verification, there may be a greater need to update the biometric template, in order to avoid too high a false rejection rate in such use.

d If biometric images are taken again at renewal, these could be used to update the enrolment template if necessary.

Recommendation 16. The system should provide the facility for updating biometric templates. In the case of face recognition, the template should be updated at each renewal.

5.2 Procedures at 'back office'

91. The back office processing in cases where there is suspicion of possible duplicate enrolment needs to emphasise ease of decision-making. A single response of the closest match is far preferable to a gallery of near misses, although if there are genuine problems of multiple similarities these should be escalated to a third stage of resolution. The aim is to achieve a clearly unambiguous result, whether it is in establishing an identity for an entitlement card, a driving licence or a passport, and whether it is a first enrolment or a renewal.

92. A policy decision must be taken on what to do in cases where a duplicate enrolment attempt is confirmed. Will any penalty be applied, or is second enrolment simply disallowed? Many of the duplicates in the Philippine SSS-ID [3] are attributed to non-fraudulent causes, e.g. people making a second application because of delays in receiving their entitlement card form their first application.

Recommendation 17. The identification system should return single identity rather than a selection of possible identities.

5.3 Remote and off-line enrolment

93. Although enrolment at high street offices or shops will be the norm, there will be situations where a remote or manual process will be required, e.g. for the housebound or disabled. Some fingerprint and iris recognition suppliers offer handheld units, which may be useful for this purpose. It might also be possible to enrol previously collected 'inked' fingerprint images, or images of the iris taken at a local opticians' site. These will present significant quality and security challenges, due to the lack of a complete audit trail.

5.4 Procurement procedures

94. Such considerations will be explored during the procurement cycle, which may take considerably longer than the purchase of comparable information technology systems due to the novel nature of these systems. A single authority building upon the lessons learnt elsewhere should be responsible for developing the specification and appropriate service level agreements. Testing and refining the specification following the analysis of the results of pilots will be an iterative process.

6 USER ATTITUDES TOWARDS BIOMETRIC IDENTITY SYSTEMS

95. With biometric methods and systems gaining maturity, and the prospect of larger scale deployments in the near future, both activist groups and individuals are voicing concerns about the societal impact of such systems. In this study we have aimed to bring together some of these observations, based upon direct evidence from deployments and managers involved in their operation, and from focus groups debating the public understanding of these new technologies. Annex 1 develops the themes in more detail, addresses other possible concerns and suggests a framework for future studies. Success of mass public deployments will depend on citizens being motivated towards making these systems work well.

6.1 Public understanding of biometrics is undeveloped

96. A series of focus groups held in the late 1990's demonstrated the understanding amongst both young and old, technically aware and those fearful of new technologies that fingerprint recognition could be used in conjunction with a PIN to secure financial transactions. In contrast, the possibility of using iris patterns was only entertained by a quarter of the subjects. Many years of exposure to the use of fingerprints by the police has given an over-inflated impression of the accuracy of fingerprint systems as applied in practical biometric-type scenarios. It may be difficult to convince citizens of the need to supply more than one fingerprint (a narrative explaining the need for a second, backup, fingerprint in case of damage to the primary finger, is likely to be accepted, although people often fail to understand that each finger has a different print and minutiae). However, considerable resistance could be encountered if systems similar to the 'tenprint' IND application (where a rolled print is taken from each finger) were mandated, or if two biometric methods were to be used. At a more basic level, the multiplicity of biometric methods has created continued misunderstanding. Confusion between iris and retinal methods is rife, and the hand geometry units at DisneyWorld are often interpreted as fingerprint units.

Recommendation 18. Clear simplified messages to the media are required, from both the biometric industry and government.

Recommendation 19. Piloting of systems in public spaces is needed, to increase familiarity with these new technologies.
(Iris and vein pattern recognition systems were demonstrated in the Millennium Dome exhibition.)

6.2 Balancing the costs and benefits

97. Using any new or additional security measure entails change in routinised actions. The greater the change or effort required, the more evident must be the benefit. The IND 'tenprint' and enrolment of individual rolled fingerprints attracts little comment by the participants, since the benefits for asylum seekers are clearly communicated. Users of this system are already primed through their peer networks and the use of fingerprints in government identity checking in their countries of origin is often already established.

98. If biometric methods are to be extended to a wider population, and enrolment centres are limited to high street locations, the costs of travel to these, together with the additional costs of adding a biometric to a passport will have to be balanced by a clear justification of benefits both to the individual and to society as a whole.

99. Those being enrolled will have questions and concerns that need to be answered by the officer who is supervising the enrolment. Clearly the longer the time allowed for this interaction, the more costly will be the process. The trade-off between spending longer on reassurance with the citizen and the resulting increased cost needs to be modelled.

Recommendation 20. An appointment system for enrolment is required to minimise waiting time.

Recommendation 21. Clarify the benefits to the individual and to society as a whole through targeted education and marketing.

6.3 Addressing the fears about use of fingerprint data by the police

100. A senior UK fingerprint examiner with many years of experience in the front line of police activities mentioned that many householders who had been burgled refused to be fingerprinted to eliminate their own prints from those of a burglar—in spite of assurances about the destruction of their data after use. In a deployment in the USA, however, we were told that assurances of limitation of use were sufficient to gain the trust of the participants. Although at present, databases of facial images are being developed and systems to convert these to templates which could be searched against a national biometric database of faces are still in early stages, facial biometrics could in due course suffer from this same concern.

101. Clearly, there are technical measures that could reassure citizens: if iris recognition were to be used, or a fingerprint system not using minutiae (not recommended in this study) were implemented. Alternatively, the database could consist of templates with no storage of unprocessed biometric images and the templates could be encrypted using one-way hash algorithms or public key systems to increase the effort required to run crosschecks against other databases. Procedural measures such as a published Code of Practice as to use by government and commercial entities could reassure other groups in the community.

Recommendation 22. Selection of the most appropriate reassurance mechanisms is required.

6.4 Addressing other concerns

102. Unfamiliarity with these novel technologies will inevitably raise concerns about detrimental effects to the individual. There are stories about iris recognition systems using a laser to illuminate the eye. In fact the system uses low-level infrared illumination, and has been show to conform to the relevant IEC60825-1.2 safety standards [15]. Even when reassured on this point, users raise questions about the long-term effects of being close to such light sources or the possibility of catching an illness through contact with surfaces touched by many people.

103. There have also been instances of intentional damage to fingerprint readers, by supervising officials as well as by the public. Of course, there are also privacy and personal data issues, but surprisingly these were not uppermost in the discussions on acceptability that have been made public.

104. Once users are informed of the possibility of the systems not being perfect, their questions centre on procedures to avoid direct accusation of fraud. Enrolment centre officials will need to be trained to respond confidently to such concerns and approach the process of resolving any ambiguities in identification in a sensitive manner.

Recommendation 23. Early and continued public education is required, together with a full analysis of all of these aspects by biometric device and system suppliers.

Recommendation 24. A secure and user-friendly process, and backup system, is required for non-fraudulent database matches.

Recommendation 25. The enrolment centre requires a private space for enrolment and follow-through in case of such matches.

7 COST

105. We estimate that including a biometric component in a national identity database will increase costs by approximately £500 million (over the originally specified 10 year rollout period). By far the largest component of this cost will be the resources expended in collection of the images for biometric enrolment. Some of the principal cost elements are shown in the following table.

Item	Unit cost	Number	Item cost
Licence fees for biometric components, software etc	£1 per person	50,000,000 people	£ 50 million
Biometric hardware at front office	£5000 per front office	2000 offices	£ 10 million
Biometric hardware for remote enrolment	£2000 per front office	2000 offices	£ 4 million
Hardware at back office, networks etc			£ 10 million
Marketing and publicity	£1 per person	50,000,000 people	£ 50 million
Enrolment (allowing 10 minutes per person)	Staff costs £40 per hour	50,000,000 * 10/60 hours	£330 million

106. Enrolment costs could be reduced if the biometric component is not used for one-to-one verification. This would save time when enrolling the biometric into the system, as there would be no need to explain and demonstrate the verification process.

8 CONCLUSIONS

107. This feasibility study concludes that:

a In principle, fingerprint or iris recognition can provide the identification performance required for unique identification over the entire UK adult population. In the case of fingerprint recognition, the system would require the enrolment of at least four fingers, whereas for iris recognition both irises should be registered. However, the practicalities of deploying either iris or fingerprint recognition in such a scheme are far from straightforward.

b Such a system would be a groundbreaking deployment of biometrics. Not only would it be one of the largest deployments to date, but aspects of its performance would be far more demanding than those of similarly sized systems; such existing systems are either not applied in the civil sector, or operate in countries where public acceptability issues are less prominent.

c Current biometric systems are not designed for civil application of the scale envisaged in the UK entitlement scheme, and further work by the biometrics industry is needed to specify how best to use either of the two technologies.

d The use of biometrics will add to the cost of an entitlement card system. The most significant component of cost is the time and effort to collect and enrol biometric data. However, this is one of the least well-understood aspects of biometric technologies. For example the types and number of exception cases will have an impact on throughput performance and choice of an appropriate back-up strategy.

e The introduction of a biometric system to limit multiple identity fraud is unlikely to be achievable by the originally suggested date of 2005. With the 2007 date suggested in the Consultation Paper, the timetable is still ambitious, but provided the background work commences as early as possible in 2003, we believe that it should be achieveable. An outline timetable for implementation in this timescale is given in Appendix A.

8.1 Selection of biometric technology

108. We have identified three alternatives:

a Implementation of a fingerprint-based system to reduce the possibility of successfully obtaining multiple identities in a national database, with a supporting facial recognition system to help resolve accidental duplicates or intentional fraud;

b Implementation of a system using iris image recognition to reduce the possibility of successfully obtaining multiple identities in a national database, with a supporting facial recognition system to help resolve accidental duplicates or intentional fraud;

c A decision not to proceed with a database that includes biometric identifiers on the grounds of the high risk of failure and/or cost overrun.

109. The fourth option of using all three biometric systems—fingerprint, iris and face—has been rejected both on the grounds of cost and inconvenience to citizens as well as on the likely perception by critics of this as being a ‘solution too far’.

110. Throughout this report we have compared fingerprint and iris recognition technologies in respect of their application to successful deployment of a national database of identities.

Appendix B summarises the key differences between these methods and their application to the UKPS/DVLA proposals

111. We believe that a decision on which technology should be used—fingerprint or iris recognition—should be deferred, pending the result of the consultation exercise and further action on the part of the UKPS and DVLA, the suppliers of biometric sub-systems and system integrators.

8.2 Further studies

112. We have identified a number of actions that are required over the next 9-12 months, to address many of the current unknowns, and help in selecting the appropriate biometric technology, and determining appropriate operational procedures.

a To determine the acceptability of biometric systems (especially fingerprint-based identity schemes), both by analysis of the numbers and strength of the responses to the Consultation Paper, and by careful, focussed research amongst opinion formers and the public at large. This requires action by the UKPS, DVLA or the Home Office.

b To encourage biometric suppliers and system integrators—particularly of iris recognition—to reduce the uncertainties in deployment of biometrics in an entitlement card system. Benchmarking of currently available technology and extensive studies to understand the range and number of exception cases are required. A roadmap of likely future improvements to the hardware and user interface is also needed.

c Further analysis of the major reference fingerprint system, the federal US IAFIS system with its 40 million database, to ascertain the key technical determinants of the success of a civil AFIS.

d Co-ordinated studies with the other members of the core European group of national authorities interested in the application of biometrics to travel documents and identity cards (Netherlands, Italy and Germany). These studies should include the development of a methodology for analysis and implementation of security measures for these systems. There should also be co-ordination with similar studies being undertaken in the USA by the Federal Aviation Administration (FAA) and National Institute of Standards and Technology (NIST).

e A further study should address enrolment strategies and associated timescales using realistic pilot implementations of commercially available iris and fingerprint units. The number of subjects should be between 500-1000 to capture a variety of problem cases. This would allow more accurate costing of the options, since people and process costs are likely to dominate this aspect of the national identity scheme. The specification and execution of this study should help in devising the larger 'exception' study where the number of participants is ten times greater.

8.3 Implementation risks

113. We summarise the major risks that could impact the viability of such a groundbreaking system are:

a **Safety.** This should be independently assessed, to demonstrate that systems are as safe as possible. Public reassurance is required, especially for systems that are unfamiliar to citizens such as those using iris recognition.

b **Security.** The identification must remain secure, firstly to ensure that it fulfils its aim of helping prevent fraudulent applications, and secondly to protect users' biometric data against misuse.

c **Excessive number of false alarms.** A false alarm occurs when the system mistakenly indicates an attempted duplicate enrolment. Such cases must be resolved manually using other slower and more costly checks. Excessive numbers of such alarms could result in a backlog of unprocessed applications. In some cases, these checks will involve face-to-face interviews at which an innocent applicant may face a false accusation of fraud. If this happens too often, public confidence in the system will be compromised. Because the false alarm rate depends on the size of the database, this problem may become apparent only once a sizeable proportion of the population is enrolled, at which point it will not be possible to change many aspects of the system.

d **Speed and ease of capture of biometric images.** There is also the potential for a bottleneck in the process of capturing biometric images of individuals. Nearly all the existing information on the speed of these processes derives from relatively small trials in which the subjects are not representative of the population as a whole. Currently, there is little understanding of the absolute numbers—and distribution in the population—of those for whom it is difficult or impossible to capture good quality biometric images. Back-up processes need to be provided for these people.

e **Public acceptance.** Attitudes of the population to the use of biometrics are not well understood. It is clear that many citizens fail to appreciate how the systems operate and are unaware of the capabilities of such systems. This lack of knowledge hinders a rational debate on the merits of the use of biometrics in national schemes, thereby allowing urban myths and intentional disinformation to affect public opinion in an adverse way.

APPENDIX A. IMPLEMENTATION ROADMAP

Date		Activities
2003	Q1	End of consultation on entitlement cards Collation of comments and opinions
	Q2	Completion of the collation exercise Internal UKPS/DVLA/Home Office decision to go ahead Start informal discussion of options with system integrators/biometric suppliers Collaboration (leadership?) with the other members of the European Travel Document Group on Biometrics Encouragement of EPSRC research submissions on methods to assess user acceptability and changing social perceptions on biometrics, together with studies on long term security (1-2 year projects only)
	Q3	Formal decision to go ahead announced 1st specification of system(s) Initial prototypes (proof of concept) for demonstrations available from system integrators Single authority identified to champion the trial and procurement process. Research starts on social acceptability, security
	Q4	Selection of the preferred partners for the trial of systems
2004	Q1	Development of piloting strategy with preferred partners.
	Q2	Preferred partners develop and produce equipment for trial 2nd specification of system based upon results of preferred partners' internal tests
	Q3	Year of trials including both technical and non-technical elements. Redesign of equipment & refinement of the specification in response to the ongoing results of the tests
	Q4	
2005	Q1	
	Q2	
	Q3	Final decision on go-ahead on entitlement card Choice between iris or fingerprint (if both technologies still appear feasible) 3rd and final specification agreed
	Q4	Procurement process (1 year)
2006	Q1	
	Q2	
	Q3	Tenders returned and adjudicated Agreement with High Street Partners
	Q4	Production of units/kiosks; Fitting out of High Street Partners' enrolment stations
2007	Q1	Final testing of the system (including real use in 2 'test' towns)
	Q2	Handover of system Marketing and publicity campaigns
	Q3	Soft launch in selected towns or region
	Q4	Launch of service in main towns and cities
2008	Q1	Second level local services for rural areas launched

APPENDIX B. FINGERPRINT AND IRIS RECOGNITION COMPARED

	Fingerprint recognition	*Iris image recognition*
Operating principle	Most systems use the minutiae in fingerprints, i.e. the ends of ridges or where ridges split into two.	Almost all systems use the same underlying method for coding and comparing the features of the iris.
Information available to establish 'uniqueness'	10 fingers, with approx 30-50 minutiae points per finger. The ring and small fingers provide less information content & there is some correlation between data from separate fingers.	2 eyes, with over 200 binary degrees of freedom in each 512-byte template. There is no evidence of correlation between two iris patterns.
Maturity of the technology	Extensive experience in its application to criminal AFIS systems—up to 40 million records in FBI database.	Over 15 years of development of the method, mostly by the one supplier. Several small scale deployments
Hardware	Many optical and electronic sensors. Large area platen sensors for 'slap' fingerprint capture of all fingers. Portable fingerprint units for remote data capture.	Specialised cameras. Improved user interfaces required and are under development. The camera system could capture a face image at the same time
Maturity of one-to-many identification	Civil AFIS systems have been implemented in several countries, though none yet of the scale or complexity of the UK application.	No examples of systems of this size and complexity;
Performance in one-to-many identification	Data from at least 4 fingers is required, 10 fingers recommended.	Identification using a single eye theoretically feasible, but use of both eyes is recommended.
Maturity of one-to-one verification	Numerous deployments; handheld units for mobile application are available	Select number of deployments Generally more expensive; handheld systems under development
Performance in one-to-one verification	Good	Very good
Security against fake biometrics	Poor, additional liveness tests need to be developed.	Satisfactory
IPR considerations	Suppliers have proprietary algorithms and matching hardware	Fundamental patents owned by Iridian.
Exceptional cases	Missing hands and fingers Difficult to register fingerprints for some sections of the population. (women, East Asians, manual labourers, older people)	Congenital eye conditions (anirida, coloboma, anophthalmia) eye damage & disease. Partial images of iris may be all that can be obtained.
Privacy implications	Concerns about access and cross-matching with criminal justice systems	
Other social and individual concerns	Hygiene issues. Reuse of electronic images of fingerprints.	Health and safety fears.
Advantages	Technology challenges now well known. Exception cases documented. Reference deployments available. Number of competing solutions.	Cannot be searched for scene-of-crime latent fingerprints. Facial photos can be captured at same time as iris images are captured. Automated quality control.
Disadvantages	Concern about access to database by police. Human element to quality control.	No large database of irises to assist in benchmarking systems. Extent and nature of exception cases need to be addressed.

APPENDIX C. LIST OF RECOMMENDATIONS

Recommendation 1. For the identification application, if a fingerprint system is used, it should be minutiae based.

Recommendation 2. Store raw biometric images to allow for future algorithm changes. These do not need to be stored with the identity database for fast retrieval.

Recommendation 3. Investigate the options for alternative, privacy-enhancing, database architectures that may offer a measure of security against duplicate issue of identity documents and responds to criticisms of comprehensive national registers.

Recommendation 4. Pilot implementations as part of the tendering and implementation process will be necessary to obtain good estimates of performance in the deployed applications.

Recommendation 5. For fingerprint recognition to uniquely identify one person in a population of 50 million at least four fingers per person are needed. Collecting prints from all fingers is recommended.

Recommendation 6. For iris recognition to uniquely identify one person in a population of 50 million we recommend using images of both irises.

Recommendation 7. Face recognition is not strong enough to uniquely identify one person in a population of 50 million.

Recommendation 8. Identity verification should use an on-card template on card, not accessing templates from the central (identification) database.

Recommendation 9. Performance of face recognition is satisfactory for watch-lists of size up to approximately 1000.

Recommendation 10. If face recognition biometrics are to be used, the face photograph should be taken at the 'front office' where it can taken in accordance with appropriate standards [6] to ensure best possible performance.

Recommendation 11. For identification, the biometric component must treat failure-to-acquire errors separately from failure to match by system.

Recommendation 12. In addition to the normal equipment and processes for biometric image capture, versions will be needed to provide additional assistance in problem cases, and for collection of the required biometrics away from the front office.

Recommendation 13. A study is required on the size and types of failure to acquire population, in order to decide the appropriate secondary methods for biometric image capture for exception cases.

Recommendation 14. If the identity system uses fingerprints, collect flat prints rather than rolled prints. Furthermore, make use of 'live-scan' electronic capture fingerprint devices in preference to the digital scanning of inked fingerprint cards.

Recommendation 15. The security of the identity database is very important. The database must be secure against fraud, and not introduce possibilities for further fraud. A security evaluation of the system must be carried out.

Recommendation 16. The system should provide the facility for updating biometric templates. In the case of face recognition, the template should be updated at each renewal.

Recommendation 17. The identification system should return single identity rather than a selection of possible identities.

Recommendation 18. Clear simplified messages to the media are required, from both the biometric industry and government.

Recommendation 19. Piloting of systems in public spaces is needed, to increase familiarity with these new technologies.

Recommendation 20. An appointment system for enrolment is required to minimise waiting time.

Recommendation 21. Clarify the benefits to the individual and to society as a whole through targeted education and marketing.

Recommendation 22. Selection of the most appropriate reassurance mechanisms is required.

Recommendation 23. Early and continued public education is required, together with a full analysis of all of these aspects by biometric device and system suppliers.

Recommendation 24. A secure and user-friendly process, and backup system, is required for non-fraudulent database matches.

Recommendation 25. The enrolment centre requires a private space for enrolment and follow-through in case of such matches.

APPENDIX D. GLOSSARY

AFIS	Automated Fingerprint Identification System, originally defined in respect of use of fingerprint to identify criminals from latent images found at the scene of crime
ANSI X9.84	American National Standards Institute standard on biometric information management and security
BWG	UK Government's Biometric Working Group, co-ordinated by the Communications Electronics Security Group on behalf of the UK e-Envoy's office
DVLA	Driver and Vehicle Licensing Agency (UK)
FAA	Federal Aviation Administration
FRVT	US Department of Defense comparison of the performance of algorithms for facial recognition; these are held regularly and distinguished by the year in which they are undertaken
FVC	University of Bologna's comparison of the performance of fingerprint algorithms
IAFIS	Integrated Automated Fingerprint Identification System the USA's federal AFIS system
ID	Identity, in the context of identity cards
IEC 60825	International Electrotechnical Commission standard on optical radiation safety
IND	Immigration and Nationality Directorate (UK)
INS	Immigration and Naturalization Service (USA)
ISO 17799	International Standards Organisation standard on information security management
NIST	National Institute of Standards and Technology (USA)
NPL	National Physical Laboratory (UK)
PIN	Personal Identification Number
Privium	A scheme for frequent travellers at Schiphol airport in which iris recognition is used to fast-track through immigration control
SSS-ID	Philippines social security application of biometrics
UKPS	United Kingdom Passport Service
UNHCR	United Nations High Commissioner for Refugees

APPENDIX E. REFERENCES

[1] KENT, S.T. and MILLETT, L.I., *Ids—not that easy: Questions about nationwide identity systems*. 2002, National Academy Press

[2] DAUGMAN, J. Biometric personal identification system based on iris analysis. *U.S. Patent No. 5,291,560* March 1, 1994.

[3] CIRIACO, M.C.C. Developing and implementing the Philippine social security ID system: A large-scale ID application using biometrics. 1999.

[4] FBI NATIONAL PRESS OFFICE, *Press release* August 10, 1999. http://www.fbi.gov/pressrel/pressrel99/iafis.htm

[5] BLACKBURN, D., BONE, M., and PHILLIPS, J. *Facial recognition vendor test 2000.* February 2001. http://www.dodcounterdrug.com/facialrecognition/FRVT2000/documents.htm

[6] MANSFIELD, A.J., KELLY, G.P., CHANDLER, D.J., and KANE, J. *Biometric product testing final report*. Report for CESG and Biometrics Working Group, March 2001. http://www.cesg.gov.uk/technology/biometrics/media/Biometric%20Test%20Report%20pt1.pdf

[7] MAIO, D., MALTONI, D., CAPPELLI, R., WAYMAN, J.L., and JAIN, A.K. FVC 2000: Fingerprint verification competition. *IEEE Trans. PAMI*, 2000, **24**(3), 402-412. Details also online http://bias.csr.unibo.it/fvc2000/

[8] MAIO, D., MALTONI, D., CAPPELLI, R., WAYMAN, J.L., and JAIN, A.K. FVC 2002: Second fingerprint verification competion. *ICPR 2002*, Quebec City. http://bias.csr.unibo.it/fvc2002/Downloads/FVC2002_ICPR.pdf

[9] CAMBIER, J. *Iridian cross-comparison test*. Iridian Technologies, Report TR-02-004 December 2002.

[10] NIST. *Use of technology standards and interoperable databases with machine-readable tamper-resistant travel documents*. Appendix A. 2002. http://www.itl.nist.gov/iad/894.03/NISTAPP_Nov02.pdf

[11] NIST. *Best practice recommendations for capturing mugshots and facial images. Version 2.* NIST Image Group, September 1997. http://www.itl.nist.gov/iad/894.03/face/bpr_mug3.html

[12] BS ISO/IEC 17799. Information technology. Code of practice for information security management. 2000.

[13] ANSI, *X9.84 biometric information management and security*. 2001

[14] MATSUMOTO, T., MATSUMOTO, H., YAMADA, K., and HOSHINO, S. Impact of artificial gummy fingers on fingerprint systems. *SPIE, Optical Security and Counterfeit Detection Techniques IV.*

[15] SLINEY, D.H., *Optical safety evaluation of the Iridian technologies LG iris access 2200 imager.* 2001