UK Biometrics Working Group

Use of Biometrics for Identification and Authentication
Advice on Product Selection

Issue 1.0

Document Status and History

Issue No	Date of Issue	Issued by	Reason for issue
1.0	November 2001	OeE	Public Release

References

	Title	Location
	Biometrics Working Group	<www.cesg.gov.uk/technology/biometrics> e-mail: biometrics@cesg.gov.uk
	the Biometric Consortium	<www.biometrics.org>
	BioAPI (Biometric Application Programming Interface) Consortium	<www.bioapi.org>
	Common Biometric Exchange File Format (CBEFF)	<www.itl.nist.gov/div895/isis/cbeff >.

Biometrics for Identification and Authentication
Advice on Product Selection – Issue 1.0

Contents

1. Introduction

1.1 Aims and Scope

1. This document specifically addresses the use of biometrics for Identification and Authentication (ID&A). In the context of this document "biometrics" is defined as "the automated means of recognising a living person through the measurement of distinguishing physiological or behavioural traits".

2. Choosing a biometric solution for a government application is often a daunting task. Faced with little reliable information about biometrics (vendors, products, and integrators), how do you go about making a sensible decision? The intent of this document is to provide sound and practical advice for government managers trying to create a solid, biometric procurement proposal or operational requirement. **The advice contained within this document is intended to supplement, not replace, accepted project management best practices and methodologies.**

3. The success or failure of a biometric system in a particular application **is not** dependent upon the reliability of the biometric product alone - and this can't be emphasised too strongly! There are many other factors that contribute to the overall success or failure of the implementation, and most of these factors will be covered within this document. It is also essential to understand that no single biometric technology offers a solution to all user requirements. Furthermore, **a biometric solution for your requirement is not always the best approach!** Often, analysis of the requirement will reveal that existing solutions are adequate, or may be enhanced by other, non-biometric means.

4. Hopefully, by giving careful thought and consideration to the topics described herein, the risk of embarking upon a project that will have little or no chance of success will be kept to a minimum. A summary checklist is provided at the end of this document with topics/questions that must be answered before proceeding with a biometric procurement proposal or operation requirement.

5. The aims of this document are:

   - to identify the issues to be addressed before a biometric based ID&A system is introduced;
   - to identify the implementation issues to be addressed after a biometric based ID&A system is chosen;
   - to provide advice on how to specify and choose a biometric based ID&A system;
   - to define some of the common terms used in biometrics;
   - to provide references to other reading matter and user groups.

1.2 Acknowledgements

6. The Office of the E-Envoy (OeE) is grateful to the UK Biometrics Working Group for producing this document. It reflects the invaluable contributions, experience, and knowledge of the members and as such, is a unique advice document. More information on the UK Biometrics Working Group can be found at www.cesg.gov.uk/technology/biometrics.

2. Biometric Selection

2.1 Background Work

7. Before embarking on any major project, it is naturally a requirement to do your homework. Understanding the impact on all of those who are affected by the system can be critical. When proposing a biometric solution for an application, the major problems are often found to be entirely legal and political:

- Are privacy issues involved?
- Who should have access to this data and for what purpose?
- Will your biometric solution be used to protect government data, and if so, have you consulted the relevant national policy for the appropriate security assurance?
- What legislation will affect the kind of information that can be stored regarding your users (e.g. Human Rights/Data Protection Acts—**this is extremely important!!**)?
- Will your user population be willing to embrace your biometric proposal?
- What standards, in terms of biometrics and information technology, are required?

8. You must uncover any legal or political obstacles to your proposed application before things progress too far.

9. Obviously, a business case will be needed to justify the expenditure for your proposal. As part of your business case, it would be wise to investigate thoroughly the 'do nothing' option. By including this information in your proposal, you may (or may not) discover that a biometric solution would be essential to your programme. In any case, reporting on this aspect will demonstrate that you have truly thought about the project from many different angles and that you are not just trying to insert biometrics into the project.

10. You may also want to investigate any other available options/alternatives by making a comparison between the security offered by passwords, tokens, and biometrics. UK government users should contact the CESG (Communications Electronics Security Group, <www.cesg.gov.uk>) in order to consult the relevant government policy regarding such a comparison.

11. When writing your procurement proposal or operational requirement, take care to describe only what is needed, not how it should be achieved (you should be driving the project, not the vendor). This allows the suppliers/vendors to tender a solution that best fits their particular hardware/software. Furthermore, put the onus on the supplier/vendor to prove to you that his/her particular solution meets your requirements.

12. Additionally, you need to develop an evaluation model to weight/score the proffered solutions **before** you have received them. Higher priced proposals may be justifiable if you fully understand the cost benefits vs. the risk analysis. Understanding how much of the supplier's solution is off-the-shelf, versus new development, is crucial to your risk analysis.

2.2 User Attitude

13. Biometric systems may be thought of as a marriage between technology and human beings. In any good relationship, if one of the partners becomes neglected/undervalued, the relationship will suffer. You cannot underestimate the human aspect of the equation in your biometric application, and you must satisfactorily find the answer to this question: how well do you know your user population?

14. The user population includes not only the actual users of the system, but also the administrators of the system and (possibly) other members of staff. **Do not** assume that you know your user population, for you may very well be unpleasantly surprised. If your users resolve to be stubborn about the use of a biometric device, for whatever reason (fear of technology, invasion of privacy, cultural abhorrence to touching things, etc.), then your application may be severely handicapped before you've even started. Clearly, user attitude can make or break the implementation of a biometric system, and past experience has shown this to be true. If at all practical, a survey of the user population that specifically addresses the attitude of the users towards the intended biometric should be conducted. It may provide essential information before the intended programme of work progresses too far.

15. If you are encountering user resistance to the project, or even **before** you encounter it, embarking on a user education programme that positively approaches the introduction of a biometric system to the user population would be time and effort well spent. Users are not necessarily enamoured with the 'enhanced security' argument, however they do like to hear how it will benefit them. Will they not have to remember a password? Will it provide faster access to something? Properly preparing your user population for a change will ease your transition into using the new biometric system. In fact, involving your user population in the project from the outset is considered to be the ideal way of ensuring the highest level of cooperation. While training and education of personnel might significantly impact the cost of your application, the value added to addressing user concerns can be of greater benefit in the long run.

16. In addition, you should also define whether the users of the system will be the customers of it (public) or your own employees (private). Attitudes toward usage of the biometric devices, which will directly affect performance of the system, also vary, depending upon the relationship between the end-users and system managers. In general, staff will tolerate minor inconveniences in order to get their jobs done, however members of the public may be far less tolerant.

17. Further user considerations include the following:

- **User Privacy Concerns** – The collection of biometric information may be the subject of privacy concerns among the target audience. Certain biometrics engender a greater perception of privacy invasion among the public than others. Also, what legal requirements must be satisfied governing the collection and storage of the information?

- **User Perception** – Public perception, which may correspond to the degree of a particular device's intrusiveness, can severely impact user acceptance of certain biometrics. For example, while retinal scanning devices (ones which use infrared technology to look at the pattern of blood vessels at the back of the eye) may claim greater accuracy than other biometrics, the perceived invasiveness of the capture device has, in the past, resulted in public reluctance to routinely use this biometric.

- **Target Clientele Characteristics** – Some biometric systems may perform better, given a target audience with a majority that possess (or don't possess) a certain feature or characteristic. For example, race, gender, occupation, age, or colour of eyes may affect the error and success rates of certain biometrics.

- **User Difficulties** – Some populations have difficulty using certain biometric capture devices. Difficulties may be encountered with the degree of alignment necessary in the feature capturing process or with certain inherent characteristics of a given target population (e.g. the elderly tend to have very dry skin, which can make adequate contact with certain types of fingerprint capture devices difficult). Disabilities within your user population must be taken into account (height of the device for wheelchair users, inability to provide a sufficiently admissible biometric feature, etc.).

- **Ease of Use** – The acquisition method for the user's biometric feature, problems with the user authentication process, and/or speed of a product can greatly influence user acceptance. Less intrusive, procedurally quick biometric systems are more likely to be successful.

2.3 Technical Issues to Consider

18. The biometric feature selected as the identifier for your users must be an accurate, relatively unalterable, distinguishing, physical or behavioural characteristic that can be captured, recognised, and authenticated over an indefinite (but certainly not infinite, due to the inevitable changes that occur through ageing, illness, or injury) period of time.

19. Furthermore, the method of capturing the biometric identifying feature should be unobtrusive to the user. The method selected must be socially acceptable and must not endanger the health, safety, or welfare of any user. The system has to be simple to use. Use of the system must be easily understood by the employees administering the system and must be simple to explain to the users.

20. Departments should contemplate the following product considerations when selecting a biometric:

- **Template Storage** – The size of each template (i.e. the information recorded representing a user's biometric features) may be a factor when selecting a particular biometric product for your application. In choosing a biometric solution, you need to consider the template size and whether multiple templates per user will be required. Multiple templates from each user (several different fingers, both eyes, face and voice, etc.) may be needed (e.g. to achieve necessary levels of system accuracy/security, to account for the accidental unavailability of a user's biometric feature, etc.). The amount of storage needed for these multiple templates may influence the viability of card storage and/or your computer processing capabilities. For example, if you choose to provide your users with a smartcard as a means of storing their biometric templates, many (but not all) biometric systems offer templates small enough to reside on a smartcard. You must be aware of the current, maximum capacity for the storage of your users' templates on whatever medium you choose (smartcards, magnetic stripe cards, various barcode technologies: 1D, 2D, and 3D; computer memory, etc.), as well as its processing power/capabilities and compatibility with the hardware involved. Security and protection of the template data is also an issue (does the level of risk or the need to protect privacy in your application warrant the encryption of templates and/or the transmission of data?). How will your solution provide for this?

- **User Population** – It is important to consider the number of users who may be prevented from using a particular biometric type (due to disability, cultural considerations, health conditions, etc.). If a large part of your user population might be precluded from using a particular biometric type, then it would be wise to choose a biometric that is more appropriate for the vast majority of your users. **You cannot expect to find a single biometric that will be accessible for all of your users, all of the time.** For example, user populations that contain large numbers of people that work hard with their hands (who may have more difficulty using a fingerprint device due to worn or dirty fingers) may want to choose something more suitable, such as facial recognition. Cultures with an aversion to touching public surfaces would prefer to use biometric solutions that are 'hands free'. Are there any items of clothing or accessories (safety masks, gloves), worn by the majority of your user population, that would make a particular biometric inappropriate for use in your application? On the other hand, certain biometrics may prove to be advantageous to users having difficulty utilising traditional access control measures. **It really pays to know your user population.**

- **Computer Resources** – The complexity of the algorithms used in matching the users to their enrolled templates may vary from product to product. Therefore the amount of computer processing power required will differ. In mainstream types of applications (i.e. those that do not require massive throughput and do not have enormous user populations), you are more likely to consider those biometrics that perform reasonably well, using a workstation with a moderately priced processor, than those that require more expensive platforms.

- **Maintenance** – All biometric devices will require some form of maintenance. The frequency and intrusiveness of periodic adjustments (possibly due to factors in the

operating environment such as lighting, background noise, dirt/grime, weather, etc.) must be taken into consideration in order to ensure correct acquisition of the biometric data. You need to be cognisant of the potential difficulties in supporting the continued and accurate use of the biometric system that you choose.

- **Biometric Upgrade/Obsolescence** – The ease with which a given biometric product can be updated/improved/replaced over time may impact your selection. Because biometric products will change over time, the implications surrounding upgrades/replacements should be seriously considered. Replacements from a different supplier are not easily done, given the current lack of interoperability amongst most biometric devices (however, with the emergence of an accepted Biometric Application Programming Interface (API) and the CBEFF (Common Biometric Exchange File Format), such issues may become less prevalent in the near future). Will this be a concern for your application?

- **Testing/Evaluation** – There is a need for uniformly recognised testing/evaluation of both performance **and** security for biometric products/systems, to ensure that reported results are calculated consistently and without bias, across all products. In the future, security evaluations that conform to Common Criteria standards may also be required. Reliable performance and security testing/evaluation results could assist in the selection of a biometric. In a perfect world, all types of biometrics would have been tested/evaluated for both their performance (under numerous applications/conditions-- i.e. the same biometric may give radically different performance results within a different type of environment or application) and for their security effectiveness. Ideally, in terms of performance evaluation, it would be prudent to require that the biometric you choose had been previously tested for performance accuracy/efficacy in an environment that closely approximates that of your application. However, to date, only some biometrics, in a limited number of environments/applications, have been performance tested, and the methods for security testing are in the trial stages. It is advisable to investigate the current testing/evaluation status for a given technology or solution, to find out if there has been a performance test/evaluation completed in an application that is similar to the one you will be proposing. If no independent performance tests or evaluations exist for a particular device, in the kind of application that you have specified, then you may want to consider: consulting an appropriate organization to acquire the proper evaluation methods (if you choose to undertake the testing within your department) or hiring an experienced, independent facility to conduct your test. Two of the leading groups for such help and information are the Biometrics Working Group (e-mail: biometrics@cesg.gov.uk) or the Biometric Consortium <www.biometrics.org>. Both are excellent sources for the latest information on independent tests/evaluations and test laboratories.

2.4 General System Requirements

21. The following generic functions are required of all biometric systems:

- the ability to add and delete users

- enrolment of the users
- data collection, which includes the capture of the user's biometric feature/characteristic presented to the sensor
- transmission of the captured data (which may include signal compression and re-expansion of the data)
- translation of the captured data into a stored record ("template")
- signal processing — where biometric information from the user's current attempt to access the system are extracted from the received signal, compared to the previously stored data in the template, and given a "score"
- an authentication policy, which makes the decision to "accept" or "reject" the user based upon the system's security criteria and the user's "score" (received from the signal processing system)
- a system security policy covering audit trail information, quality control, and system management issues

2.5 Enrolment Issues

22. You will need to define some sort of enrolment policy for all of the tasks and procedures associated with enrolment. In addition, you may need to consider having a separate system solely dedicated to the purpose of user enrolments. The answers to the following questions should be included within the policy that you define:

- What user data will you require along with the enrolled template (e.g. name, age, gender, etc.)?
- How long should enrolment take for each individual?
- How many attempts at enrolment will be allowed?
- How long will an enrolled template be considered valid, since a user's biometric information will change/age over time? Oftentimes, only experience can tell you this, but one can always initially define a system administration policy for user template re-enrolments/updates based upon some reasonable expectations.
- If a user cannot contribute a valid template for enrolment, due to either a temporary or permanent situation, what work-around measures have you defined?
- Will the enrolment database need to allow for the backup of stored information and easy recovery?
- Or will there be no centralised database, requiring each user to carry his/her biometric data on a portable storage medium, such as a smartcard?

- What security/protection for the enrolled template data needs to be provided?

2.6 Cost

23. The cost of implementing **and maintaining** the entire system package will certainly affect your choice of biometric. It is essential to build a solid business case for your proposed solution. Outline the reasons for the project, the objectives, and the benefits gained. Thoroughly understand the costs and consequences of 'doing nothing' (i.e. maintaining the status quo) and include this information within your business case.

24. Even though the costs associated with purchasing a piece of biometric hardware are generally decreasing, the cost of building the supporting infrastructure is still a barrier for many. Emerging developments in the areas of infrastructure may have a significant impact on biometric pricing. Consequently, it is important to consider modularity at the application interface in order to allow the interchange of commercially developed hardware components.

25. Another question that must be considered is whether there are any alternatives to a biometric identifier that can be used to reduce or eliminate the problem you are trying to address (passwords, magnetic stripe cards, etc.). Forcing a biometric to fit into your application may not be the best choice that could be made. **Fascination with the technology is not a sufficient business case.** Investigating your other options may save you a lot of hassle in the long run.

26. Likewise, selecting a vendor before you have written a proposal is not a good idea. **The allure of a particular product is not a sensible selection criterion.** The vendor should be chosen to fit your specifications—not the other way around. Define your application, write the proposal, and make the competing vendors sign up to your requirements in their bid.

27. Your costing research should determine the costs of the biometric solution in terms of hardware, software, maintenance, personnel, training, and impacts on existing procedures, versus the cost of a different option. Further questions dealing with cost are included on the checklist provided at the end of this document.

2.7 Positive or Negative Identification

28. Defining how you want the users of your biometric system to be authenticated by the system will be one of your most important decisions. Biometric systems can be configured to run in either a 'positive' or a 'negative' identification mode, and for certain applications can be tasked to do both.

- Positive identification: proving I am someone enrolled in the system.
- Negative identification: proving I am not already enrolled in the system.

29. In a positive identification system, you will first be asked to identify yourself — by providing a pin number, a password (which could be something simple, like your

name), or by presenting a token containing your identity information, such as a swipe card or a smart card. Then you present your biometric characteristic, and it is compared to your biometric template (i.e. the biometric information, unique to yourself, that was stored at the time you enrolled). Positive identification systems minimise the possibility that you will be linked to another record, because **you** have specified (by giving it your pin, password, etc.) which record you want to be compared with. (Note: positive identification is also roughly, but not exactly, equivalent to 'one-to-one matching' and/or 'verification' in the industry parlance.)

30. Positive identification applications are used to try and prevent multiple users from claiming a single identity. In such applications, there are numerous alternatives to biometrics, including ID cards, PINs, passwords, etc. The use of biometrics can be a voluntary choice, since there are other alternatives for recognition of the user.

31. The opposite of a positive identification is a negative identification. In a negative identification system, the new user claims **not** to be currently enrolled in the system. Therefore, upon the initial enrolment, the new user's enrolment template is matched against all users in the system who appear to be similar, to ensure that a duplicate does not exist. (Note: negative identification is also roughly, but not exactly, equivalent to 'one-to-many matching' and/or simply 'identification' in the industry parlance). It is not usually necessary to make comparisons against every enrolled template, because clearly there are going to be users that have such disparate looking templates that it would be futile to make the comparison. Most vendors account for this variation between users by categorising, or 'binning' the templates into like groupings, so that incoming biometric information need only be compared to the information in the group or groupings that are most similar.

32. Negative identification applications are most often found in implementations where it is illegal for a single person to have multiple, registered identities on the system (e.g. in driver licensing and social service eligibility systems). Apart from the "honour" system, where each person's word or documentation is accepted, there are no reliable, alternative methods to biometrics for proving that the user is not already registered in the system. The use of biometrics in negative identification applications must be mandatory.

33. The following table provides a brief outline of positive and negative identification:

POSITIVE	NEGATIVE
To prove **I am** someone **registered** on the system	To prove **I am not** someone already **registered** in the system
Comparison of submitted sample to a **single** claimed template	Comparison of submitted sample to **multiple,** similar looking templates to look for a possible duplicate

34. It is fairly common for biometric systems in government applications to perform both functions—i.e. negative identification at the time of enrolment (to prevent the issuance

of multiple identity documents for a single purpose/service), and positive identification at the point of service (to prevent access to these services by non-enrolled users).

35. Will the biometric system in your particular application be used for positive identification, negative identification, or both? If both functions are required, will they be required from the same biometric measure, or do you wish two measures to be used (e.g. fingerprint for the negative identification and voice for the positive, etc.)? It is extremely important that the answers to these questions be specified within the description of the biometric system desired in your procurement or operational requirement document.

2.8 Cooperative versus Non-cooperative Users

36. This terminology refers to the behaviour of the potential 'bad guy' or deceptive user. In positive identification applications, such as access control, the deceptive user is cooperating with the system in the attempt to be recognised as someone s/he is not (e.g. "Mike" knows that "Joe" is a valid user on the system. Mike masquerades as Joe to try and gain access to Joe's privileges or account information). Users in cooperative applications may be asked to identify themselves in some way, perhaps with a card or a PIN, thereby limiting the database search of stored templates to that of a single claimed identity. This is what we call a "cooperative" application.

37. In negative identification applications, the bad guy is deliberately not cooperating with the system in an attempt not to be recognised. This may be because the person knows or believes that he/she may already be enrolled on the system (e.g "Mike" has some underlying incentive to want duplicate access or benefits from the system, so he will try to "look" different for the system to establish a second identity), or because the person has some reason for not wanting to be enrolled in the system's database. This we call a "non-cooperative" application. Users in non-cooperative applications cannot be relied on to present themselves correctly, thereby requiring comparison against others previously enrolled in the database (which could turn out to be a fairly large task).

38. The motivation of your user population, whether cooperative or non-cooperative, will contribute in some way to your overall system performance. Therefore it is recommended that you clearly describe which type of deceptive motivation, cooperative or non-cooperative, that you expect to encounter in your application.

2.9 Habituated/Non-habituated Users

39. Defining the habituation level of your users in your procurement or operational requirement document will give the contractor/vendor a better idea of how to prepare the final system for your particular user population. Your proposal must address the frequency with which the intended users of the system will actually be presenting themselves for biometric recognition—multiple times per day? Weekly? Monthly?

40. What many people fail to recognise, or simply to understand, is that there is a learning curve associated with each type of biometric technology employed. The more often a user accesses a particular biometric device, the more practised the user becomes, and

the less likely it will be that the machine will fail to recognise that person. This is because the user has grown more consistent in presenting his/her biometric feature.

41. Biometric devices all require a certain degree of consistency in the presentation of the user's biometric feature, and some devices may require a higher degree of cooperation and user involvement/accuracy to achieve this than others. You will need to address the training aspects of your user population in your proposal.

42. Users presenting a biometric trait on a daily basis can be considered habituated after a short period of time. Access control to your work area or to your computer is generally "habituated". Users who have not presented the trait recently can be considered non-habituated. Access control to a social service benefit provided on a monthly basis is generally "non-habituated". For the most part, your users will be "non-habituated" during the first weeks of operation, and thereafter your application will have a mixture of habituated and non-habituated users at any given time.

2.10 Supervised/Unsupervised Application*****

43. This refers to whether the use of the biometric device during operation will be observed and guided by system management (e.g. human security guard or computer) or not. In unsupervised applications, the temptation exists for someone to try to attack or invade the system, however this scenario may pose little or no threat for your application.

44. Non-cooperative applications will generally require supervised operation, while cooperative operation may or may not. Nearly all systems supervise the enrolment process, although there are some that do not. All personnel involved in the enrolment of users will require training in detection of the fraudulent techniques that may be employed by the users.

2.11 Open/Closed System

45. Will the system be required, now or in the future, to exchange data with other biometric systems run by some other management (open)? Or will the data be kept within your own application, not to be shared with any other management (closed)?

46. For example, some US social service agencies want to be able to exchange biometric information with other States. Since this system is to be open, data collection, integrity/protection, compression, and format standards are required, as well as mutual agreements/requirements for data use (taking privacy legislation into consideration), in order to facilitate the exchangeability of the information between agencies. If you have any intent in the future to share information between agencies or systems, it is much easier and more cost effective to build these considerations into your application prior to implementation.

2.12 Standard/Non-standard Environment

47. If the application will take place indoors at a standard temperature (20^{o} C), a standard pressure (1 atm.), and under other reasonably established environmental conditions

(particularly where lighting or noise conditions need to be controlled), it is considered to be a "standard environment" application. Outdoor systems, and perhaps some unusual indoor systems, are considered to be "non-standard environment" applications.

48. The application's environment can have a profound effect on the performance of the equipment and the stability of the user's biometric characteristic. It is important to specify clearly any environmental conditions that would differentiate the application from a standard, office type environment. Will the temperature vary greatly? Will the lighting vary due to sunlight streaming in from a nearby window, possibly affecting the image acquisition of the biometric? Is there a significant amount of background noise that might affect sound-based (voice recognition) systems? If there are any unusual environmental conditions within your application, it is essential that these be stated within the procurement or operational requirement document. In any case, the biometric device(s) should be able to be adapted to the environmental conditions in the application(s) for which the biometric will be used. If not, you could possibly consider a different biometric, otherwise, you should investigate your non-biometric options.

2.13 Overt versus Covert Usage

49. If the user is aware that a biometric feature is being measured, the use of the biometric is overt. If unaware, the use is covert. The use of biometric systems for covert applications presents a number of legal issues and technical considerations that are quite unique. It should be ensured that any such proposed implementation follows all statutory requirements.

50. Almost all conceivable access control applications are overt. One fairly well-known and (mostly) covert application of a biometric is the facial recognition system employed in the Newham shopping district of London, which uses CCTV cameras to provide images of the passers-by, in order to compare them with images of known pickpockets and thieves. Although there are signposts throughout Newham warning the public that this system is in operation, an individual does not necessarily know if or when his/her face has been captured by the system.

51. It should also be pointed out that a deceptive user cannot cooperate (or noncooperate) with a biometric system unless the application is overt. Although it may seem fairly obvious which type of application you will employ, it would be beneficial to specify this clearly in your procurement or operational requirement document.

3. Biometrics Performance Factors

3.1 Introduction

52. The performance of a biometric system is usually stated in terms of its false acceptance and false rejection rates, the rate of user throughput, as well as other metrics. Such measures of performance are generally dependent on the application, the user population and their behaviour and motivations, as well as on the environment.

53. This section briefly lists the user and environmental factors that have been found to affect performance. Such a list can be useful when considering or implementing biometric systems, to ensure that possible problems have been considered. It is also of use when evaluating system performance, suggesting factors that may need to be controlled or recorded during the data collection phases. The information has been extracted from a report by the National Physical Laboratory.

54. Each of the factors listed will generally cause problems with only a subset of biometric technologies. For example illumination changes affect only optical based systems (e.g. those based on Face, Fingerprint, Retina, Iris or Vein imaging), while acoustic noise would affect sound based systems (e.g. Speaker verification). Moreover, some biometric devices operate in a way to control the effects of any problems. Equally, problems may be observed that are not included in our lists.

55. When problems arise, generally the effect is to reduce the likelihood of an attempt matching an enrolment template, thereby increasing the false rejection rate. However, in some cases, noisy or problem images can allow spurious false matches and an increase in the false acceptance rate.

3.2 General influences

56. With most biometric systems differences in performance will be observed depending on the age, gender, ethnic origin of the user, their familiarity with the system and motivations in using it, and on the time elapsed since enrolment. The observed differences may be due to more fundamental factors, listed in later sections.

- **Age.** Children (who change more rapidly) and older people (where perhaps minor damage to the measured biometric takes longer to heal) tend to have more false rejections than average.

- **Ethnic origin, Gender and Occupation** (e.g. clerical, manual, maintenance). The quality of a person's biometric (for a particular biometric system) may depend on their ethnic origin, gender and occupation. A biometric system "tuned" to a specific target population may perform less well if used with a different ethnic or gender mix.

- **Template ageing** (i.e. the time elapsed between creation of the enrolment template, and the verification or identification attempt). Generally, performance a short time

after enrolment, when the user appearance and behaviour has changed very little, is far better than that obtained weeks or months later.

- **User familiarity.** As users become familiar with the system, they are more likely to position themselves correctly, and to know the appropriate action to compensate for many of the verification problems that might arise.

- **User motivation.** Users will act differently according to the importance of the biometric transaction.

3.3 User based influences

57. User based influences may be based on physiology, behaviour and appearance attributes. These influences are listed below together with the influenced biometric.

User Physiology

- Beards, moustaches (Face)
- Baldness (Face)
- Disability: e.g. amputees, blind users, users in wheelchairs or on crutches
- Eyelashes (Iris)
- Fingernail growth (Fingerprint, Hand)
- Fingerprint fineness - Depth and spacing of ridges
- Fingerprint condition - Dry, cracked, damp
- Height (Face, Iris, Retina) - The very tall or very short, or those in wheelchairs may have difficulty in positioning themselves
- Illness, medical conditions, or medication: Amputees, Arthritis (Hand, Fingerprint), Blindness (Iris, Retina), Colds (Voice)
- Deterioration or improvement in medical conditions
- Iris colour intensity (Iris)
- Skin tone (Face, Iris)

User Behaviour

- Dialect, accent, native language (Voice)
- Expression/intonation/volume (Voice)

- Facial expressions (Face)
- Misspoken or misread prompted phrases (Voice)
- Movement (Face, Iris, Retina), Lack of movement (Gait, Face)
- Pose, Profile, quarter-profile (Face, Gait), Head tilted (Face, Iris, Retina)
- Positioning, Offset and rotations, (Finger, Hand). Distance from camera, high, low, to one side (Face, Iris)
- Previous user activity, Out of breath (Voice), Sweaty (Fingerprint), Swimming may result in shrivelled fingers (Fingerprint)
- Stress/Tension/Mood/Distractions

User Appearance

- Clothing - Hats, earrings, scarves, (Face). Sleeves (Hand), Trousers, Skirts (Gait), Heel height (Gait, and Face due to change in subject height)
- Contact lenses (coloured, patterned) (Iris)
- Cosmetics (Face)
- Glasses, sunglasses (Face, Iris)
- False fingernails (Hand, Fingerprint)
- Hairstyle or hair colour changes (Face)
- Rings, plasters, etc. (Hand, Finger)

3.4 Environmental influences

58. Environmental influences are based on general background, lighting, ambient noise and weather conditions. These influences are listed below together with the influenced biometric.

- Background, Colour, Clutter (Face), Containing other faces (Face)
- Lighting, Level (Face, Iris, Vein), Direction (Face, Iris, Vein), Reflections (Face, Iris, Vein)
- Background Noises (Voice), Other voices in background (Voice)
- Weather, Temperature, Humidity, (Fingerprint, Vein), Rain & Snow (Face, Fingerprint)

3.5 Device influences

59. Device influences result from the sensor itself or the interface with users:

- Sensor and Hardware
- Dirt/smears. On camera lens (Face, Iris, Retina) or on sensor or platen (Hand, Fingerprint)
- Focus
- Residual fingerprints on sensor
- Sensor Quality. Microphone quality (Voice)
- Sensor replacement
- Sensor variations. System might have different types of sensor. Sensor may change over time
- Sensor wear
- Transmission channel. Noise Variation

User Interface

- Feedback given to users
- Quality of instruction to users

4. Pearls of wisdom

60. This section will cover things learned en route by others that have already completed biometric procurements. It is sound advice that should be adhered to if at all possible.

61. In general, the most successful biometric implementations are ones that replace existing, underperforming systems—systems that were deemed either too expensive/problematic to the administrators or too cumbersome to the users. You are most likely to succeed where the biometric provides a faster, cheaper, and easier access for all concerned. Success may also be based upon the willingness of the system management to assess the alternatives and to do the work necessary to make the systems effective, if initially faltering.

4.1 Hardware

62. There are many aspects surrounding hardware issues that will need to be addressed within your procurement or operational requirement document. Questions such as:

- What hardware is already available within the application?
- Will interoperability be an issue between your existing hardware and the proposed system?
- Will it be necessary to provide backward compatibility with any existing system(s)?
- Will there be a need for flexibility within the system to handle additional biometrics or future services/requirements?
- Will there be a need to exchange data between other agencies that may not be using equipment from the same biometric vendor?

63. Currently, there is little or no interoperability between biometric systems, even those utilising the same biometric characteristic (but produced by different vendors). The BioAPI (Biometric Application Programming Interface) Consortium is working to address this situation, and has proposed a standard that is largely being taken up by the biometric industry. Progress is being made, but widespread compatibility/ interoperability has not been achieved to date. Visit the BioAPI website, <www.bioapi.org>, for the latest information on the status of these efforts.

64. The Common Biometric Exchange File Format (CBEFF) is also being developed to facilitate biometric interoperability. CBEFF describes a set of data elements necessary to support biometric technologies in a common way, addressing the data interchange between different system components (or systems), the forward compatibility for technology improvements, and the simplification of the software/hardware integration process. CBEFF examines the security information (such as digital signatures and data encryption), processing information (e.g. the biometric type), information about the

biometric sample, and the biometric data itself. The latest, official information on CBEFF can be found at <www.itl.nist.gov/div895/isis/cbeff >.

65. The following extract is a slightly modified version of a paragraph contained within the US Government's General Services Administration Smart Access Common ID Card: Final Requirements Document, dated July 2, 1999. It provides a reasonable example of how you might wish to state your flexibility requirements.

"The platform must be designed to allow for the timely, economical, and easy addition of new application modules as they are identified by the agencies, without impacting existing functions. The design must be flexible and must not rely on a single component supplier or product in such a way that a necessary change or upgrade to the platform would result in a significant loss of investment, a degradation of performance, or require the support or use of an unreasonable amount of agency resources. The design should incorporate off-the-shelf components whenever feasible so as to reduce risk and investment in new development."

66. At the bare minimum, you will need to state all of the currently owned equipment, computers, servers, software, etc. that can or will be put to use within your requirement, in order to assist the vendors or the integrators with their proposals and, ultimately, to end up with an overall system/package that works within your requirements.

67. Realising that the best-laid plans almost never run smoothly, you should consider a phased implementation of your biometric solution. Putting the entire system into place all at once will undoubtedly create some problems that hadn't even occurred to you (hardware **and** software integration issues will always crop up). By implementing your system in manageable phases, you can work through each set of problems that occur before facing the next ones. It may also be beneficial to tie vendor/integrator payments to the successful completion of each phase, defining specific criteria (test procedures or metrics) that is required to be met in order to confirm the successful completion.

4.2 Quality Control

68. Enrolment quality is the key to achieving satisfactory operational performance of the biometric system. The environment under which an enrolment is taken *will* affect the quality of the enrolment (for example, noisy backgrounds for voice devices, poor lighting for face systems, excessive heat/cold, wetness, etc.). Furthermore, the environment and equipment under which subsequent access attempts are made should replicate the enrolment conditions as closely as possible, or you can expect to see some degradation in the performance of your system. For example, with voice recognition systems, if the level of background noise is significantly different from when the user enrolled to when the user normally accesses the system, or if the biometric system's acquisition sensor differs significantly between enrolment and access attempts (different camera makes/models, microphone vs. telephone handset, telephone vs. mobile/cell phone, etc.), then you can expect performance failures at a higher rate.

69. Additionally, simply changing the position of a device (e.g. wall mount vs. table setting) between enrolment and access (or between access attempts) can dramatically affect

performance. Determine the environmental factors that will affect both the enrolment quality and subsequent access attempts, then try to sensibly achieve the right balance for the best possible performance. A list of potential sensitivities of biometric devices has been included within this document.

70. Feedback on poor enrolment quality at the time of enrolment is also important to a successful implementation. What sort of quality control feedback will the vendor offer on the enrolment? The success or failure of your application may depend upon having an enrolment officer with a good understanding of what an acceptable quality enrolment looks like, or receiving good feedback from the enrolment software, **or both** — state your requirement(s) for this!

71. At the very least, the enrolment capturing device must provide on-site, immediate notification of whether or not an acceptable biometric sample has been obtained, thereby guarding against the need for users to make return visits to the local enrolment offices solely to provide useable template information.

72. If an enrolment officer is required, you will need to address the issue of training — will the vendor provide the proper training or not? Will the training require extensive, specialist knowledge of the biometric feature and the workings of the entire system? How much or how little training will your personnel need (this includes users as well as system managers)? What about the ongoing needs for training of new staff? Ensuring that proper enrolment occurs, by educating both the users and the system managers, is paramount to having a properly running system.

73. To ensure that optimal quality of the captured biometric feature is maintained, the biometric capture device, either by itself or in communication with a workstation, must be capable of periodically performing automatic self-diagnostics and calibration. This applies to capture devices used in enrolment and at the point of access by the user.

74. The biometric capture device must be able to support extensive quality assurance capabilities including:

- Ability to perform an automatic assessment of the quality of each biometric sample submitted for enrolment and to notify the enrolment officer that the biometric data entered is either acceptable or unacceptable for use in performing a match;
- Ability to allow the enrolment officer to re-enter biometric input data and modify any client record data prior to creating the enrolment template; and
- Ability to flag the input data as being of poor quality and include the best of a predetermined number of presentations of the biometric feature in the enrolment record (no more than a certain percentage of all presentations may be flagged as having poor quality).

4.3 Throughput Rates

75. Depending upon the application, throughput rates may be of significant importance. Questions such as:

- How many people do you need to get through the device(s) in what amount of time?
- What are your throughput rate requirements for both enrolment and operational use?
- Will the device(s) see continuous use throughout the day or will there be "peak" times? If so, define the "peak" times.
- Are long queues/waits tolerable? If not, state your requirements to facilitate steady traffic flow.
- What effect will users that are unable to use the biometric have on your throughput rate, especially if human intervention is required?

76. Additionally, user rejections, normally requiring human intervention, may further slow usage of the device and the resulting mean throughput rate.

77. The following is provided as an example of a generic throughput rate statement contained within a procurement document: *"The system shall be configured so as to provide commercially acceptable response and throughput times for all transactions."* However, it is recommended that you state this information as specifically as possible within your procurement or operational requirement document, citing exact time figures where relevant.

4.4 Error Tolerance

78. Asking a system to perform 100% accurately, 100% of the time is clearly unachievable. Machines are prone to inaccuracy, just as the human beings using them are. That said, what sort of error tolerance could you **reasonably** expect and require from a biometric system?

79. There are two, main types of errors that can occur within a biometric system: false match and false non-match (roughly, but not exactly, equivalent to 'false acceptance' and 'false rejection' in industry parlance). The false match occurs when a person is identified as someone other than him/herself on the system (thereby allowing access to the system under another identity or allowing an unauthorised user access). You need to decide whether the probability of a falsely matched user (impostor) will be low enough to deter the (perceived) fraud in your application.

80. A false non-match occurs when the biometric system fails to recognise a properly registered user, thereby denying the user access. Due to the ongoing changes in everyone's body, errors can occur in the direction of failure to recognise a valid user, perhaps at a rate of a few percent. Failures can also occur when the user does not present his/her biometric feature properly to the capture device.

81. Of these two types of errors, false match and false non-match, it is important to state what sorts of numbers you can **realistically** and sensibly tolerate. Note that being realistic does not allow the statement of a tolerance for zero errors, of either type. That level of perfection, as has already been stated, is unachievable (and be suitably sceptical of vendors quoting such figures). Being realistic does allow for some general figures to be included within your procurement or operational requirement document. For instance, state that the application will not tolerate more than 5% of the user attempts to access being falsely non-matched and not more than 1-2% of the total user population being falsely matched (or whatever you think your application can sensibly allow). System administrators must balance the false match rate versus the false non-match rate to ensure adequate security, while remaining cognisant of user convenience.

82. The vendor ultimately chosen to implement your biometric system needs to be held accountable to some reasonable sorts of error tolerance numbers for the overall system. By not stating your error tolerance requirements, you may be leaving the implementation wide open to unacceptable levels of failures. If you find it difficult deciding upon reasonable, sensible numbers, perhaps talking to experts within the Biometric Working Group or Biometric Consortium would be helpful.

83. Questions that need to be addressed in your requirement document include:

- What sensible figures for both of these types of errors can you tolerate?
- Will the user be given additional attempts to try and be recognised?
- What will you define as the tolerable rate of occurrence for false non-matches that require intervention by trained staff?

4.5 User Fallibility

84. Realising that a certain percentage of your users will inevitably fail to be recognised by the biometric system, you must have plans to cover such situations. Furthermore, there are always some people that are chronically unable to use any system, who must be given alternate means of authentication. For people that habitually have difficulty in being accepted by a system, it may be possible to lower the acceptance threshold for that particular user to permit a greater chance for entry. However, there are inherent security risks in this approach, which need to be fully understood prior to such a policy being adopted. In general, a user whose threshold has been weakened in this way should never be told that this has occurred.

85. You must clearly define/state the procedures that will be used to authenticate the user in the absence of the availability of the user's biometric feature (due to injury, physical disability, etc.). It is crucial that these back-up measures be included as part of your procurement or operational requirement proposal.

4.6 Equipment Failure

86. The system must be reliable, allowing your application to provide uninterrupted service to its users. In the event of equipment failure (or perhaps maintenance needs), it would be wise to require adequate back-up procedures that will ensure the continuity of your system in the event of a temporary disruption in operations.

87. Additionally, it may be prudent to detail policies and assign responsibilities to ensure that appropriate contingency and disaster recovery plans are developed and maintained. Contingency planning consists of the advance plans and arrangements necessary to ensure continuity of the critical functions of the system. A contingency plan should describe the actions to be taken, the resources to be used, and the procedures to be followed before, during, and after any unlikely event occurs that would render inoperative a function supportive to the system. Such planning should also include procedures and availability of equipment for both automated and manual procedures. It would also be wise to specify acceptable response times for repairs. Would having certain replacement parts in-house be beneficial? Also, what guarantees for the (long-term) availability of replacement parts should you address?

4.7 System Security

88. To ensure adequate security, there should be common roles defined by the procurement/operational requirement document about the biometric system to include, but not be limited to:

- a security officer/security operator
- auditor/audit trail requirements
- enrolment officer/supervisor
- administrator/system manager/owner
- standard user
- VIP owner/user

89. Also, have you considered the consequences to the operation of your system if personnel critical to the operation of it are absent? Depending upon the nature of your proposed application, having ‘back-up’ personnel or deputy administrators may be required.

90. The system should support a lockout or alarm threshold for excessive invalid access attempts. This could mean locking out that particular user (perhaps even all users), or sending an alert/alarm to a supervisor, or requiring additional authentication information from the user (an additional biometric feature, a password, an ID number, etc.). Depending upon your application, you may wish to have certain ‘liveness’ detection features incorporated in to your system to deter the introduction of copies or ‘fakes’ of a

biometric feature. Also, depending upon your application, the level of risk involved or the amount of privacy required may warrant the need for the encryption of the stored templates and/or the transmission of any data.

91. In addition, the system must have a method of capturing, storing, and reporting certain management information as required, such as:

- time, date, ID, and matching score of all/certain user attempts
- the storage of images or pertinent data on failed attempts
- the number of new biometric records accepted,
- the number of biometric records verified,
- the number of users the system was unable to enrol,
- measurements of the quality of the information captured,
- system down time,
- the system errors by type,
- the average enrolment processing time on a daily, weekly and monthly basis.

92. It is also suggested that you address the possible usage of tamper deterrence and tamper indication technologies for the system itself and the information stored on it. Changes to an enrolled template or the data associated with an enrolled template, and any changes in user access rights (particularly an increase in access rights) should be flagged by your audit trail. Furthermore, does the system need to guarantee the integrity and security of the data? Does the transmission of the data (between the biometric sensor and the computer, between the computer and the database, between the computers on a network, etc.) need to be secure?

4.8 Track Record

93. Having the 'best' biometric device on the market will not ensure a successful implementation. There are too many factors affecting the overall performance and implementation of a biometric system to guarantee that installing the best technology will automatically translate into success. An enormous influence on the end performance of your system will be the effectiveness of the integrator who installs and supports your implementation. When it comes to selecting the final vendor/integrator, do your homework. Talk to the customers of the vendor/integrator and find out how pleased/displeased they are with the service provided (be aware that the biometric industry is still relatively 'young'—finding people or companies that have extensive experience with implemented biometric systems may not be easy). Will the vendor/integrator respond quickly and efficiently to trouble calls? Have they been able to successfully implement a similar instance of your particular type of biometric

system? Have customers with similar applications been successful? Will there be vendor support to accommodate wider implementation and projected growth? Once again, while not guaranteeing success (there are simply too many variables and assumptions to be made in each particular application), the feedback from the administrators of similar biometric applications will be of enormous value to your selection process.

4.9 Final Thoughts

94. If you haven't already done so, it might be a good idea to consult with the Biometric Working Group (e-mail: biometrics@cesg.gov.uk) as a sanity check. The members just might be able to provide some information or feedback that could be vital to the success of your programme. Additionally, the Biometric Consortium, a US government-based organisation, is also a very helpful resource. Its website at <www.biometrics.org> has a wealth of information, including a list of vendors with links to their respective homepages. Posing questions to the Biometric Consortium's listserv, is also a practical means of gaining advice. Membership to the listserv doesn't cost anything, and instructions for becoming a listserv member are available from the Biometric Consortium's Website.

95. Keep in mind the following issues:

- There are alternatives to biometric identification in positive identification applications.
- All security systems, biometric or otherwise, require time, money, and energy to set up and administer/maintain properly.
- System throughput rates must be carefully addressed, for both enrolment and operational use.
- Remember that the need for enrolment sessions/training for all users is (almost) always a given.
- Despite the fact that studies of user attitudes show a strong preference towards the acceptance of biometric technology, there will **always** be users who object to the use of it—what policy have you defined to address this?
- Choose your system integrator carefully. Hardware/software integration will prove to be the hardest task. Biometric technologies are not very adept at 'plug and play'. Furthermore, expect system integration to require changes in other pieces of hardware and software and track record of the technology vendor. Products and vendors are in a continual state of flux. Look for stability.
- If the finished implementation is not more efficient than the alternatives, then the use of the biometric will be seen as a mistake.

Appendix A
Biometrics Checklist

The answers to the following questions discussed within the body of this document need to be investigated and, where applicable, the results should be included in your procurement or operational requirement document

Background Work

a. Have you investigated the alternatives to the biometric solution for your problem (do you really need biometrics)?

b. What legal/political issues could hinder your programme (privacy, data access, etc.)?

c. What legislation will affect the kind of information that can be stored regarding your users (e.g. Human Rights/Data Protection Acts - this is extremely important!!)?

d. Similarly, what security/privacy requirements need to be addressed for the storage of biometric/user data, both locally and centrally?

e. Will your biometric solution be used to protect government data, and if so, have you consulted the proper national policy for the appropriate security assurance?

f. What standards, in terms of both biometrics and information technology, are required?

g. Have you addressed the issues of ease of use of the biometric by both users and system administrators?

h. Have there been any tests/evaluations of biometric systems similar to your particular application?

i. Have you talked with administrators of biometric projects similar to yours?

j. Have you done your homework on the potential vendors/integrators who have submitted for your proposal?

k. Have you developed an evaluation model to score the proposal with?

l. Do you fully understand the risks and the cost benefits?

m. Have you discussed your proposal with knowledgeable members of respected groups such as the Biometrics Working Group or Biometric Consortium?

Enrolment Issues

a. Have you defined an enrolment policy?

b. Will you need an additional station for enrolment?

c. Will the enrolment need to be supervised?

d. Do you need to establish enrolment template storage size(s)?

e. How long should enrolment take for each individual?

f. How many attempts at enrolment will be allowed?

g. If a user cannot contribute a valid template for enrolment, either temporarily or permanently, what work-around measures have you defined?

h. How long will an enrolled template be considered valid, since a user's biometric characteristic(s) change/age over time?

i. Will the enrolment database need to allow for the back up of stored information and easy recovery?

j. Will there be no centralised database because each user will be required to carry his/her biometric data on a portable storage medium such as a smartcard?

k. What security/protection will be provided for the enrolled templates?

l. Will the system use more than one instance of captured biometric input data to create the enrolment template (i.e. take several readings of the biometric characteristic and combine these readings to create the user's template)?

m. Will multiple templates per user be required (e.g. do you want to store templates for more than one finger, both the right eye and the left eye, etc.)?

n. Will the enrolment database need to have the capability to handle back-ups and perform simple recovery procedures?

o. What sort of quality control and feedback will the vendor offer on the enrolment?

p. What level of training will supervisors of enrolment need?

q. Will a human operator have the ability to intervene in the enrolment process in order to establish a better enrolment record?

r. Have you determined the environmental factors that will effect both enrolment and access attempts?

s. Have you carefully considered the list of biometric sensitivities in this document?

Technical Considerations

a. What sort of computer resources do you envision will be needed to support your overall system?

b. Will the ability to upgrade or replace your system have a big impact on your choice of vendor?

c. Have you addressed user data collection, data capture, data transmission, data translation, signal processing, authentication policy, template storage, and user management features?

d. What is the cost of the biometric solution in terms of hardware, software, personnel, training, and impacts on existing procedures?

e. Have you listed the available hardware for the application?

f. Will interoperability of the biometric system with other existing, non-biometric, systems within your application be an issue?

g. What about backward compatibility?

h. Is flexibility desired?

i. Are upgrades possible with a minimal amount of fuss?

j. Will there be a need to exchange data between other biometric systems utilising the same biometric characteristic?

Cost Issues

a. What factors are most likely to increase costs of the system?

b. What are the likely costs for making the system mandatory to all, as opposed to making it optional?

c. What are the benefits of having a biometric system likely to be? In terms of:

d. cost

e. “non-monetary” or social benefits

f. speed of operation

g. security

h. control

i. staffing

j. safety

User-related Considerations

a. Have you surveyed your user population as to the attitude towards using a biometric? A strongly negative response should indicate a reformulation of your plans or a proactive education programme.

b. Have you considered educating your users to allay their doubts/fears about implementing a biometric?

c. Will your users be employees, customers, or both?

d. What is the degree of public acceptance/user perceived intrusiveness of the intended biometric?

e. Does the majority of your target user population have characteristics that could pose disadvantages (or advantages) for your chosen biometric system?

f. Will the deceptive user be cooperative or non-cooperative in your application?

g. What types of fraudulent user scenarios can you foresee?

h. Will your users be habituated, non-habituated, or a mixture of both? If both, what is your best estimate for percentage of users in each case?

i. What will the vendor/integrator need to do to prepare the system for your particular mix of users?

j. Have you addressed the aspects of training the users on how to properly use the system?

k. What user data will you require to be stored (e.g. name, age, gender, etc.)?

Operational Issues

a. Will the biometric system in your particular application to be used for positive identification, negative identification, or both?

b. If both positive and negative identification are required, will they be required from the same biometric measure, or can two measures be used (e.g. fingerprint and voice, face and voice, etc.)?

c. Will the system be open or closed?

d. Will the system operate in a standard or non-standard environment? If non-standard, list the non-standard conditions.

e. Will the biometric measurement be overt or covert?

f. During operational use, will the system automatically flag poor quality biometric input data? How much of the input can you reasonably tolerate to be flagged as poor quality data?

g. What are your throughput rate requirements for both enrolment and operational use?

h. How many false match errors can you tolerate?

i. Will the probability of a false match be low enough to deter fraud?

j. How many false non-match errors can you tolerate?

k. In the case of a false non-match, will the user be given additional attempts for recognition?

l. What will you define as the tolerable rate of occurrence for false non-matches that require intervention by trained staff?

System Administration Concerns

a. Did you define back-up methods for user authentication in the cases of equipment failure and/or temporary unavailability of the user's biometric feature?

b. Is an appropriate contingency plan and disaster recovery policy important to the success of your programme?

c. What guarantees for repair response times and replacement parts should be addressed?

d. Have you defined the roles of a security officer/security operator, auditor/audit trail requirements, administrator/system manager/owner, standard user, and VIP owner/user for your application?

e. Have you defined substitutes or back-ups for personnel critical to the operation of the system?

f. Have you addressed training requirements for your users and system administrators, not just for the initial start of the programme but also for the ongoing training of new staff?

g. Does the biometric capture device have the capability to perform automatic self-diagnostic and calibration tasks (for both enrolment and operational use), or will the system administrator have to attend to this periodically?

h. Does the system support a lockout threshold for excessive invalid access attempts?

i. Does the audit information need to include any or all of the following: the number of new biometric records accepted, the number of biometric records verified, the number of users the system was unable to enrol, the quality measurements for the

captured biometric data, the amount of system down time, the kinds of system errors by type, and the average enrolment processing time on a daily, weekly, and monthly basis?

j. Have you investigated the possible usage of tamper deterrent and tamper indicative technologies for your system?

k. Will your audit trail flag changes to an enrolled template, the data belonging to an enrolled template, or any changes in user access rights as a safeguard against tampering?

l. Must the system guarantee the integrity and security of the data it holds and transmits?