PAS 92:2011

Code of practice for the implementation of a biometric system

Publishing and copyright information

ISBN 978 0 580 69851 4

ICS 35.240

Publication history

First published June 2011

Contents

Foreword ii
0 Introduction iii
0.1 Aim of this PAS iii
0.2 About recognition systems iii
0.3 About biometric systems iii
0.4 Uses of biometric systems v
1 Scope 1
2 Terms and definitions 1
3 Assessing the need for a recognition system 5
4 Determining the type of recognition system to use 6
5 Planning for the implementation of a biometric system 8
5.1 General 8
5.2 Biometric modality 8
5.3 Performance parameters 9
5.4 Security 12
5.5 Usability 13
5.6 Accessibility 13
5.7 Data capture 15
5.8 Exception handling 18
5.9 Privacy and data protection 19
6 Acceptance testing a biometric system 21
7 Operating a biometric system 22
7.1 Legislation 22
7.2 Maintenance 22
7.3 Change management 22
7.4 Management information system data 23
7.5 Fallback arrangements 23
Annexes 24
Annex A (informative) Basic principles of a biometric system 24
Annex B (informative) Relationship between security and false acceptance rates 27
Annex C (informative) Examples of security risks and countermeasures associated with a biometric system 28
Annex D (informative) Data protection principles 29
Bibliography 30

List of figures
Figure 1 – Relationship between a biometric system and a recognition system for a specific application iv
Figure 2 – Components of a simple biometric system v
Figure 3 – Relationship between the performance parameters of a biometric system and its application 10
Figure 4 – Example of trade-off between FAR and FRR for different threshold levels 10
Figure A.1 – Components of a biometric system 26

List of tables
Table B.1 – Resistance to attack potential related to FAR 27

Foreword

This Publicly Available Specification (PAS) was commissioned by the UK Department for Business, Innovation and Skills (BIS). Its development was facilitated by the British Standards Institution (BSI). It came into effect on 22 June 2011.

Acknowledgement is given to the following organizations that were involved in the development of this guide as members of the Steering Group:

- BSI Consumer & Public Interest Network
- Fujitsu
- Home Office Science – Centre for Applied Science and Technology (previously Home Office Scientific Development Branch)
- IBM
- IBS
- Identity and Passport Service (IPS)
- KeCrypt Systems
- Morpho UK Ltd
- National Physical Laboratory (NPL)
- National Policing Improvement Agency (NPIA)
- Phoneability
- UK Government Biometrics Working Group (BWG)
- Co-opted

Acknowledgement is also given to those organizations and individuals that submitted comments during the public consultation.

This PAS is not to be regarded as a British Standard. It will be withdrawn upon publication of its content in, or as, a British Standard.

The PAS process enables a specification to be rapidly developed in order to fulfil an immediate need in industry. A PAS may be considered for further development as a British Standard, or constitute part of the UK input into the development of a European or International Standard.

Use of this document

As a code of practice, this PAS takes the form of guidance and recommendations. It should not be quoted as if it were a specification and particular care should be taken to ensure that claims of compliance are not misleading.

Any user claiming compliance with this PAS is expected to be able to justify any course of action that deviates from its recommendations.

Presentational conventions

The provisions of this PAS are presented in roman (i.e. upright) type. Its recommendations are expressed in sentences in which the principal auxiliary verb is "should". The recommendations are presented in colour-shaded boxes to distinguish them from supporting text.

Supporting text is given in the form of commentary, explanation and general informative material, which does not constitute a normative element.

Spelling conforms to The Shorter Oxford English Dictionary. If a word has more than one spelling, the first spelling in the dictionary is used.

Feedback

Feedback on the technical content of this PAS can be submitted through the BSI Document Feedback system http://feedback.bsigroup.com.

Any feedback received will be reviewed when developing future revisions of this document.

Contractual and legal considerations

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Compliance with a PAS cannot confer immunity from legal obligations.

0 Introduction

0.1 Aim of this PAS

This PAS is intended for organizations considering the procurement and implementation of a biometric system.

It provides recommendations and guidance that such organizations can follow to demonstrate good practice in their implementation.

In particular, it helps organizations decide whether to procure a biometric system, which one to procure, what performance requirements are needed and how to maximize the chances of a successful implementation. It also aids organizations in understanding their duties in respect of the use of biometric data.

0.2 About recognition systems

Recognition of people goes back a long way using non-automated means, either through familiarity or through the use of documents. Large scale automated recognition of people has only become possible since the invention of the computer. This advance has created efficient and convenient applications that were not previously possible.

A recognition system includes the management and processes to support the recognition of people as well as the actual recognition mechanism. The mechanism could be a biometric system, a password or PIN system, a token system or a combination of systems.

A recognition system is normally part of a broader application, such as a time and attendance system. The application will also have its own associated management and processes.

The collective management and processes of the biometric system, recognition system and the application will in practice not have clear demarcation and can often consist of the same personnel and be described in the same supporting documentation.

The relationship between a biometric system and a recognition system for a given application is shown in Figure 1.

0.3 About biometric systems

A biometric system is an integrated set of components (including a sensor and a matching algorithm) that automatically recognizes individuals based on their behavioural and biological characteristics. Examples of characteristics include fingerprint, voice, iris structure and face shape.

Biometric systems recognize an individual by comparing their biometric sample with one or more previously enrolled biometric references. This is achieved by:

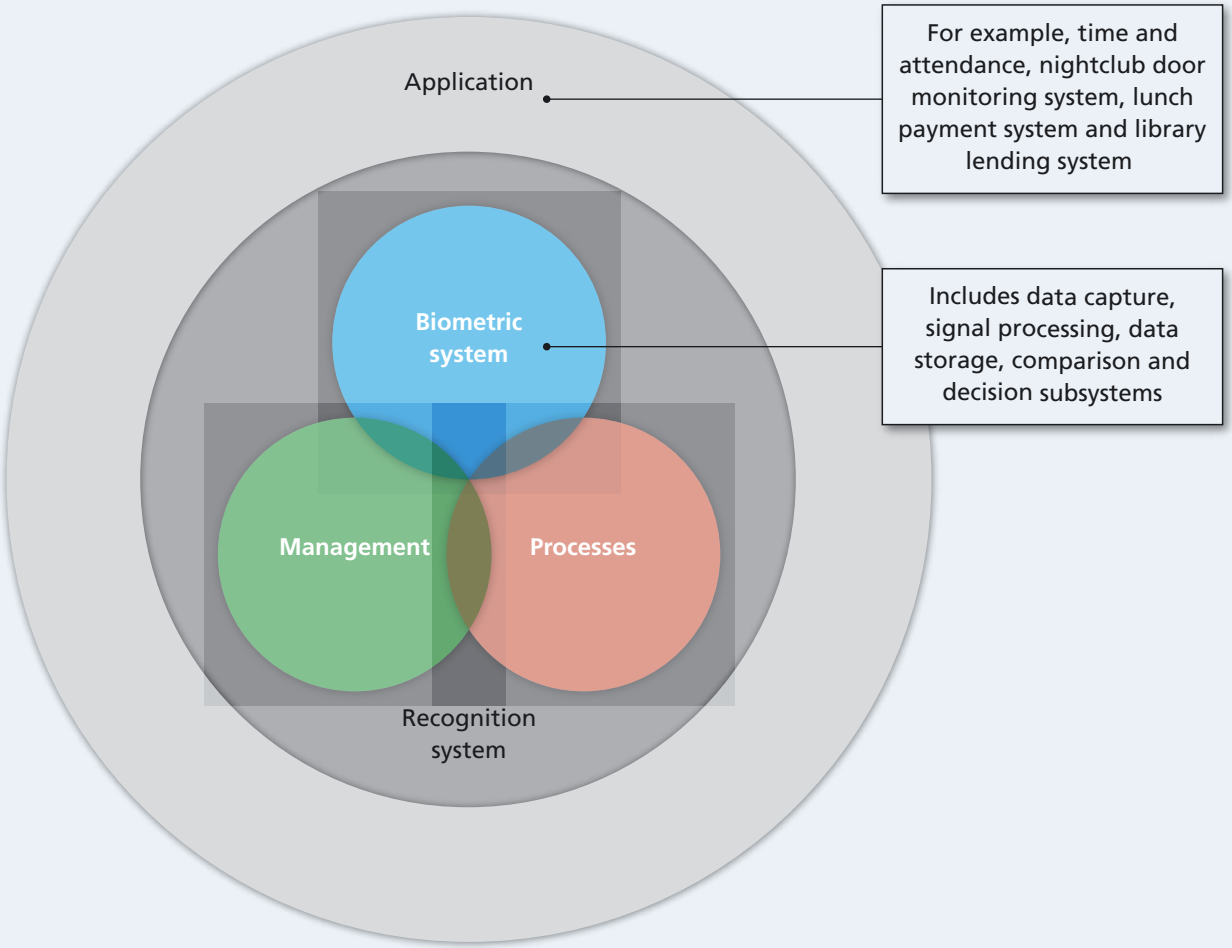
- capturing a biometric sample from an individual;
- extracting and processing the biometric data from that sample;
- storing the extracted biometric data;
- comparing the biometric data with data contained in one or more previously enrolled biometric references;
- computing how well they match; and
- indicating whether a sufficient match has been achieved.

The components of a simple biometric system are shown in Figure 2 and more detailed information on the basic principles of a biometric system is given in Annex A.

A biometric system will usually be a component of an application that requires the recognition of individuals. The relationship between a biometric system and a recognition system for a given application is described in **0.2**.

A biometric system, in comparing biometric data, does not actually identify individuals. Any perception of identity is only ever obtained by reference to some earlier registration and enrolment process where non-biometric data are collected and linked to the biometric data. It is therefore more accurate to use the term biometric recognition rather than identification and for that reason this PAS will use recognition as the preferred term.

Figure 1 – Relationship between a biometric system and a recognition system for a specific application



Biometric recognition differs from other recognition methods such as smart cards, photo ID, PINs, passwords or memorable information (e.g. birth date or mother's maiden name). It uses biometric characteristics that are strongly linked to the individual being recognized (the "subject", e.g. customers accessing a service, employees gaining access to a building and people obtaining lunches in a canteen). This provides a high level of confidence in the recognition of the person. It can also be achieved with the subject separated in space or even in time from the organization performing the recognition task. In certain applications this can allow people to receive services remotely, in a faster, more convenient manner while not revealing personal details.

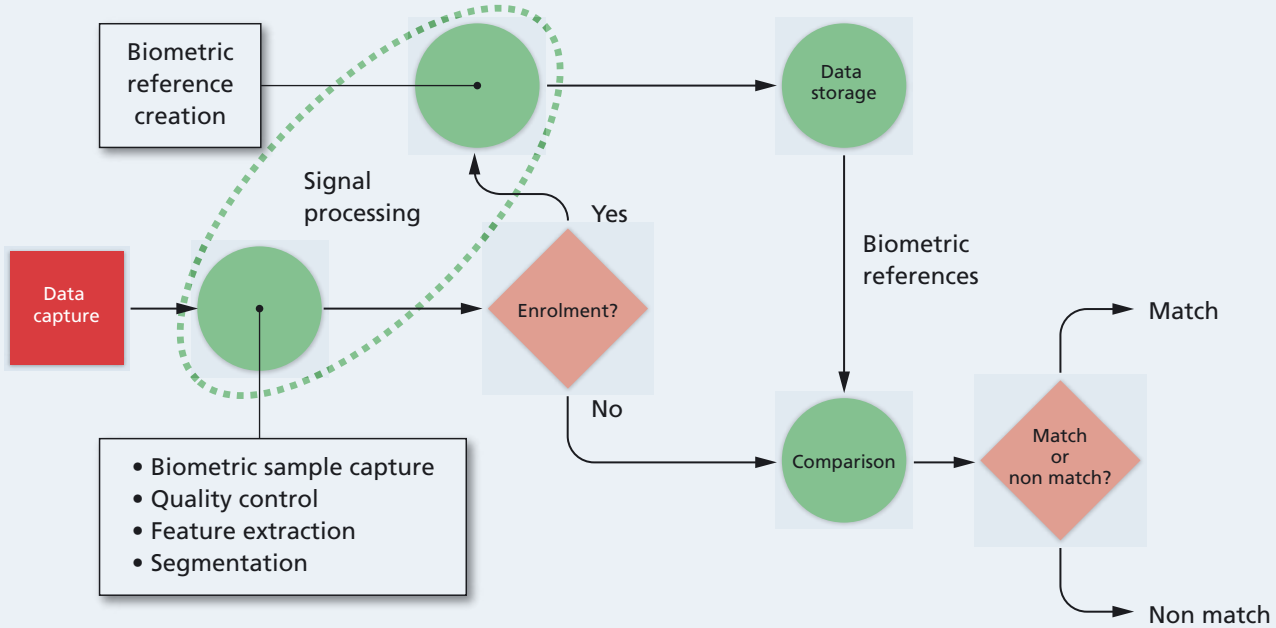
Despite the advantages of biometric recognition, biometric systems have raised public concerns. These centre on:

- fears that biometric data could be used for purposes other than those consented to by the subject, for example, providing an unauthorized link between different applications resulting in unforeseen consequences for the subject;
- fears that biometric data will not be held securely; and
- the perception that medical or other sensitive information could be obtained from biometric data.

The Information Commissioner has also highlighted the lack of clarity regarding the handling of biometric data, particularly in respect of those individuals who cannot give informed consent.

Biometric data like other personal data are open to misuse and consequently there is a need for the implementation of a biometric system to be conducted in accordance with good practice to reduce and manage any risks of abuse. This PAS provides organizations with that good practice advice.

Figure 2 – Components of a simple biometric system



Key
- Input to the biometric system
- Processing subsystem of the biometric system
- Decision subsystem of the biometric system

0.4 Uses of biometric systems

Biometric recognition of individuals is employed today in a wide range of applications. Many uses are concerned with linking a person to their privileges, such as allowing access or giving permission.

Biometric systems have been introduced in a number of types of facilities in the UK, for example, in:

- government facilities;
- schools;
- factories and offices;
- hospitals and health centres; and
- construction sites.

Applications include:

- payment for school lunches;
- purchases from self-service terminals;
- borrowing from libraries;
- access to buildings or computer systems;
- time and attendance systems; and
- access to equipment or medication.

This page deliberately left blank.

1 Scope

This PAS provides recommendations and guidance for the implementation of a biometric system. In particular, it provides recommendations and guidance on:

a) assessing the need for a recognition system (see Clause **3**);

b) determining the type of recognition system to use (see Clause **4**);

c) planning for the implementation of a biometric system (see Clause **5**);

d) acceptance testing a biometric system (see Clause **6**); and

e) operating a biometric system (see Clause **7**).

This PAS focuses on the specific aspects related to inclusion of a biometric system at the core of a recognition system where the recognition of people is an important requirement of an application.

This PAS is applicable across a wide range of applications that incorporate a biometric system. However, it is mainly directed at small- and medium-sized self-contained systems, typically those implemented by commercial organizations or local authorities.

It is also equally applicable to off-the-shelf applications that incorporate a biometric system such as a time and attendance system, as well as bespoke applications where the biometric system requires integration with other systems.

2 Terms and definitions

For the purposes of this PAS, the following terms and definitions apply.

2.1 access control

function to determine whether to grant an individual access to resources, facilities, services or information based on pre-established rules and specific rights or authority associated with the requesting party

2.2 accessibility

possibility for everyone, regardless of physical capability or technological readiness, to access and use technologies and services

[derived from PD ISO/IEC TR 24714-1:2008, **2.1**]

2.3 application

set of interrelated components and processes designed to perform a specific function

2.4 attack potential

measure of the effort to be expended in attacking an IT system, expressed in terms of an attacker's expertise, resources and motivation

[BSI ISO/IEC 15408-1:2009, **3.1.5**]

2.5 attendant

individual employed to directly interact with a subject to assist in the operation of a biometric system

2.6 authentication

process of establishing an understood level of assurance that the claimed identity of a subject is genuine, in a manner that is acceptable for the intended purpose

2.7 biometric characteristic

biological and behavioural characteristic of an individual that can be detected and from which distinguishing, repeatable biometric features can be extracted

NOTE 1 *The use of the word individual is restricted to humans.*

NOTE 2 *Biological and behavioural characteristics are physical properties of body parts, physiological and behavioural processes created by the body and combinations of any of these.*

NOTE 3 *Distinguishing does not necessarily imply individualization.*

NOTE 4 *Examples of biometric characteristics are Galton ridge structure, face topography, facial skin texture, hand topography, finger topography, iris structure, vein structure of the hand, ridge structure of the palm, retinal pattern and handwritten signature dynamics.*

2.8 biometric claim

claim that a subject is or is not the bodily source of a specified or unspecified biometric reference

2.9 biometric identification

identification by searching a database for all biometric references that match a submitted biometric sample

NOTE 1 *Also known as a 1:n comparison.*

NOTE 2 *Biometric identification can be closed-set or open-set. Closed-set identification is when the subject is known to exist in the database. Open-set identification is when the subject is not guaranteed to exist in the database.*

2.10 biometric modality

type of biometric characteristic utilized by a biometric system and the mode with which the biometric characteristic is compared against a biometric reference

NOTE *For example, facial image recognition and fingerprint recognition.*

2.11 biometric recognition

automated recognition using biometric characteristics

2.12 biometric reference

one or more stored biometric samples attributed to a subject and used for comparison

2.13 biometric system

integrated set of components that perform biometric recognition

NOTE *Components that make up the biometric system include, amongst others, a sensor and a matching algorithm. The components of a simple biometric system are shown in Figure 2 and more detailed information on the basic principles of a biometric system is given in Annex A.*

2.14 biometric verification

verification by attempting to compare a submitted biometric sample with one or more previously enrolled biometric references

NOTE *Also known as a 1:1 comparison.*

2.15 data capture device

device that collects a signal from a biometric characteristic and converts it to a captured biometric sample

NOTE 1 *A signal can be generated by the biometric characteristic or generated elsewhere and affected by the biometric characteristic, for example, face illuminated by incident light.*

NOTE 2 *A device can be any piece of hardware and supporting software and firmware.*

NOTE 3 *A data capture device can comprise components such an illumination source and one or more biometric sensors.*

2.16 data controller

person who either alone or jointly or in common with other persons determines the purposes for which and the manner in which any personal data are, or are to be, processed

[Data Protection Act 1998]

NOTE 1 *A data controller must be a person recognized in law, that is to say:*

- *individuals;*
- *organizations; and*
- *other corporate and unincorporated bodies of persons.*

NOTE 2 *A data controller will usually be an organization but can be an individual, for example, a self-employed consultant. Even if an individual is given responsibility for data protection in an organization, they will be acting on behalf of the organization, which will be the data controller.*

2.17 data subject

individual who is the subject of personal data

[Data Protection Act 1998]

2.18 enrolment

process of collecting one or more biometric samples from an individual, and the subsequent construction of a biometric reference

2.19 failure to enrol (FTE)

failure to create a biometric reference for an eligible subject in accordance with an enrolment policy

2.20 false acceptance

acceptance of a biometric claim that ought to have been rejected

2.21 false acceptance rate (FAR)

number of false acceptances as a proportion of the total number of biometric claims that ought to have been rejected

2.22 false rejection

rejection of a biometric claim that ought to have been accepted

2.23 false rejection rate (FRR)

number of false rejections as a proportion of the total number of biometric claims that ought to have been accepted

2.24 identification

act of attributing a known identity to an individual

2.25 identity

list of attribute values of an individual that allows this individual to be distinguished from other individuals within a context

2.26 impostor

subject who attempts to be matched to someone else's biometric reference

2.27 match

decision that a biometric characteristic and a biometric reference are from the same individual

2.28 non match

decision that a biometric characteristic and a biometric reference are from different individuals

2.29 performance parameter

quality metric which characterizes a particular aspect, capability or attribute of a system

NOTE *The quality is usually quantified by a numerical value.*

2.30 personal data

data which relate to a living individual who can be identified from those data, or from those data and other information, which is in the possession of or is likely to come into the possession of the data controller

[Data Protection Act 1998]

2.31 recognition system

system for the recognition of an individual using distinguishing data provided by the individual

2.32 re-enrolment

process of establishing a new biometric reference from an individual who has previously been enrolled

2.33 replay attack

attempt by a person to appear to be a legitimate user of a system by submitting data acquired during a previously legitimate transaction by someone else

2.34 spoofing attack

attack on a biometric system by an unauthorized person that uses artefacts to allow the perpetrator to masquerade as a specific authorized individual

NOTE 1 *Examples of artefacts include false fingers, photographs and voice recordings.*

NOTE 2 *Use of an artefact to avoid being recognized as someone already enrolled in the database would not generally be termed spoofing but disguise.*

2.35 subject

individual who provides biometric data or biographical data for storage, processing or comparison, or about whom such data is collected by others

2.36 threshold

numerical value, or set of values, that define the boundary between a match and a non match so that a decision can be made about whether a match or non match has been achieved

NOTE *The threshold can be adjustable to alter the decision boundary between a match and a non match.*

2.37 transaction

discrete event between an entity and service provider that supports a business or programmatic purpose

2.38 usability

extent to which a product can be used by specified individuals to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use

[PD ISO/IEC TR 24714-1:2008, **2.8**]

3 Assessing the need for a recognition system

3.1 An assessment of the need for a recognition system should be conducted. The assessment should:

a) define the business problem for which a recognition system is being considered;

b) describe why the problem requires the recognition of individuals;

c) determine the risks associated with incorrect recognition of individuals;

d) list all factors that might constrain any solution; and

e) identify the statutory requirements that might apply to any solution.

3.2 An assessment of how stakeholders, including potential subjects, might respond to the use of a recognition system should be conducted to identify potential issues and solutions prior to implementation.

The business problem for which the recognition system is being considered could be a new one or an existing one. In the latter case, if the existing problem is a result of an existing system that is deemed to be unsatisfactory, the shortcomings of the existing system will need to be identified and properly addressed in the definition of any potential replacement recognition system.

Typically, this definition of the problem will focus on abuses or shortcomings of an existing system or process. Examples of abuses and shortcomings could include: the clocking in and out of employees by their colleagues, the sharing of passwords to IT and other facilities, and the inadequate supervision of access to controlled areas.

Factors that would be useful to document as part of defining a business problem include:

a) typical and peak volumes of individuals expected to use the recognition system, as well as when peaks might occur;

b) expected population characteristics of individuals expected to use the recognition system, such as age, occupation, disability and culture;

c) the importance of the recognition process to the application and the consequences of getting it wrong;

d) the likely reaction of stakeholders to the implementation of a recognition system; and

e) the security risks associated with the business problem and how a recognition system can help address these risks.

4 Determining the type of recognition system to use

4.1 An assessment of a range of recognition systems should be conducted to identify which systems can offer solutions to the business problem.

4.2 An assessment of each of the recognition systems identified as offering a solution should be conducted to determine which system offers the most effective solution to the business problem. The assessment should:

a) determine whether the link between an individual and the credential used to recognize that individual (i.e. binding strength) is strong enough in order to address the business problem; and

b) justify the amount and type of personal data that the recognition system would need to collect in order for it to function.

All recognition systems utilize one or more of three factors to recognize an individual. These are:

- something you know (e.g. a password or PIN);
- something you have (e.g. a token, such as a smart card); and
- something you are (e.g. a biometric characteristic).

Each factor has its own particular advantages and disadvantages. Recognition systems sometimes use a combination of these factors to mitigate the disadvantages.

Disadvantages for:

- passwords and PINs include, for example, vulnerability to social engineering attacks and general misuse by subjects;
- smart cards include, for example, vulnerability to loss and theft; and
- biometric characteristics include, for example, vulnerability to spoofing.

Everyday transactions are commonly authenticated using a combination of a smart card and a PIN. Such recognition systems are taken to provide some level of assurance that the person conducting the transaction is the person identified by the smart card. This kind of authentication assurance is called indirect because neither the possession of the smart card nor the knowledge of the PIN establishes a direct link to the individual presenting the smart card, it merely indicates that the person has possession of the smart card and knows the PIN. The strength of the linkage between the authentication credential and the person is often termed the binding strength and in this case the binding strength is regarded as relatively weak because an impostor could acquire the smart card and might get to know the PIN.

Focusing on the advantages of biometric recognition, authentication using such recognition has an inherently stronger binding strength because the biometric characteristic used as the authentication credential is bound directly to the person in the form of, for example, their fingerprint, facial image, voice or signature. Authentication using biometric recognition is therefore of most interest in applications where it is of particular importance that the recognition provides a strong assurance the person present is the person enrolled.

In many instances recognition systems do not require stronger binding to an individual because, for example, the cost is small if the wrong individual is recognized, additional protection mechanisms are in place or the risk to property, computer networks or corporate reputation is small. However, biometric recognition is often used to enhance security and protect against the risk of abuse.

The binding strength between the biometric characteristics of an individual and their identity and privileges formally registered in the system is central to enhanced confidence in the permission and access validation processes.

Biometric recognition can provide other benefits too in the areas of convenience and usability. Biometric recognition can eliminate the need for organizations to issue smart cards and for individuals to carry them around. It can avoid the need for people to remember PINs and passwords, often multiple passwords, and it can overcome the security risks associated with people writing down passwords and leaving them where others can find and use them.

In some applications there might be a need to restrict each individual to a single identity record. Where this is the case, biometric recognition is a reliable method of proving that a subject is not already registered in the system, thus protecting against the creation of multiple identities within a system.

Something which is often overlooked when focusing on recognition system capabilities is the amount of personal data collected. It is important to assess what personal data will be collected and to justify its collection. Biometric systems can reduce the amount of personal data collected for recognition purposes. Therefore, in its simplest form, an application which incorporates a biometric system might only record biometric data and a storage record identifier.

5 Planning for the implementation of a biometric system

5.1 General

Stakeholders, including potential subjects, should be engaged at an early stage when preparing for the use of a biometric system in order to communicate the reasons for its use and to identify and address any concerns, particularly in relation to privacy and data protection.

Planning for the implementation of a biometric system shares many of the considerations associated with planning for the implementation of any recognition system. Some of the key factors to be considered are outlined in **5.2** to **5.9** and include:

a) biometric modality (see **5.2**);
b) performance parameters (see **5.3**);
c) security (see **5.4**);
d) usability (see **5.5**);
e) accessibility (see **5.6**);
f) data capture (see **5.7**);
g) exception handling (see **5.8**); and
h) privacy and data protection (see **5.9**).

These factors are included because they are either specific to a biometric system or important in addressing the ethical concerns raised when introducing such a system. Note that some factors, such as cost and project risk, are not discussed in detail in this PAS as they are general considerations that could equally apply to the implementation of any technology.

Whilst these factors are listed separately for convenience, they are interdependent and, as such, cannot be considered in isolation. Therefore, planning for the implementation of a biometric system is a process of selection and trade-off, with trade-off decisions being made on the basis of finding the right balance between all these factors through an iterative process.

In addition, proper consideration of all these factors, without prior engagement with stakeholders could result in the selection of a biometric system that fails to deliver the results for which it is intended. Therefore, stakeholder engagement is highlighted here as an important factor to be considered at an early stage in planning for implementation.

The success of a biometric system is critically dependant upon the extent to which users want it to succeed, and in this regard is probably more vulnerable to adverse "user reactions" than most types of technology. "Users" in this context includes not only the subjects whose biometric characteristics will be used, but also attendants, administrators, supervisors and those who have to maintain the biometric system.

A shared understanding of the business problem and the anticipated benefits is clearly a significant element in this engagement, as is a shared appreciation of the risks, both real and imagined. Individual judgements on acceptability are also influenced by their views on the value these benefits can give them as individuals.

A biometric reference cannot be verified in the same way as text data. A subject's trust in the accuracy of the biometric system is improved if the registration system demonstrates that the biometric reference is linked to the correct biographic data and/or privileges.

Acceptance with users will include factors such as concerns about privacy, protection of personal and sensitive data, and function creep. It will also depend on the usability of the biometric system and perceived confidence in its performance.

5.2 Biometric modality

An assessment of the range of biometric modalities available should be conducted in order to determine which modality to use for the intended application. The assessment should identify:

a) suitability to the target subject population (e.g. whether there are any constraints);
b) the level of subject interaction with the biometric system (e.g. whether contact with the data capture device is required);
c) the suitability of the environment in which data capture device will be located;
d) required performance parameters (see **5.3**);
e) the implementation risks (e.g. project and technical risks); and
f) the costs, both initial and on-going (e.g. maintenance and upgrade costs).

There are a number of biometric modalities that could be considered. For example, for access control, these could include:

- hand geometry;
- fingerprint;
- finger vein;
- palm vein;
- facial image;
- iris image;
- dynamic signature; and
- voice recognition.

All of these modalities are available commercially and have been deployed as part of a variety of access or workflow applications.

All biometric modalities have particular considerations that could have a bearing upon selection and, as discussed in **5.1**, choosing the right biometric modality for the application entails optimizing trade-offs between numerous conflicting factors such as convenience to users, security requirements, acceptance by users and costs.

One consideration, for example, is whether the preference is for a biometric modality that requires contact or non-contact technology. Fingerprint and hand geometry modalities are generally implemented by contact technologies, whereas facial image, iris image and palm vein modalities are generally implemented by non-contact technologies.

Another consideration might be whether the preference is a biometric modality that requires behavioural characteristics or biological characteristics. Dynamic signature and voice recognition modalities are considered as behavioural characteristics, whereas fingerprint, facial image, iris image, hand geometry, finger vein and palm vein modalities are considered as biological characteristics.

5.3 Performance parameters

5.3.1 The level of performance required of a biometric system and its associated application should be identified and described in terms of performance parameters, including:

a) error rates, for example:
   1) false acceptance rate (FAR);
   2) false reject rate (FRR);
   3) failure to enrol (FTE);
   4) application FAR (App-FAR);
   5) application FRR (App-FRR);

c) throughput volumes and rates; and

d) exception handling volumes.

5.3.2 The level of performance required should be documented alongside a justification for the level chosen.

5.3.3 Where any performance parameters used to describe the performance of a biometric system under consideration are unclear, an explanation of the parameter should be sought from the supplier.

The performance of a biometric system and its application is generally described in terms of error rates, throughput volumes and rates, and exception handling volumes. The relationship between the performance parameters of the biometric system and its application are shown in Figure 3.

The most commonly quoted error rates are the biometric system false acceptance rate (FAR) and false rejection rate (FRR), which are interdependent as shown in the example of Figure 4. A biometric system usually allows a threshold to be adjusted to provide a trade-off between the acceptance and rejection of a match. The most appropriate trade-off for a specific application will depend on the relative importance of security, convenience and cost for the application.

When a biometric system is used in an access control system, it is generally considered that the FAR relates to security and that the FRR relates to convenience. In practice, the situation is more complicated in that too many false rejections can result in false rejection fatigue and a lowering of defences against rejection of actual impostors. The FRR is probably more important than the FAR in most applications and more likely to give rise to operational problems and user rejection.

Figure 3 – Relationship between the performance parameters of a biometric system and its application

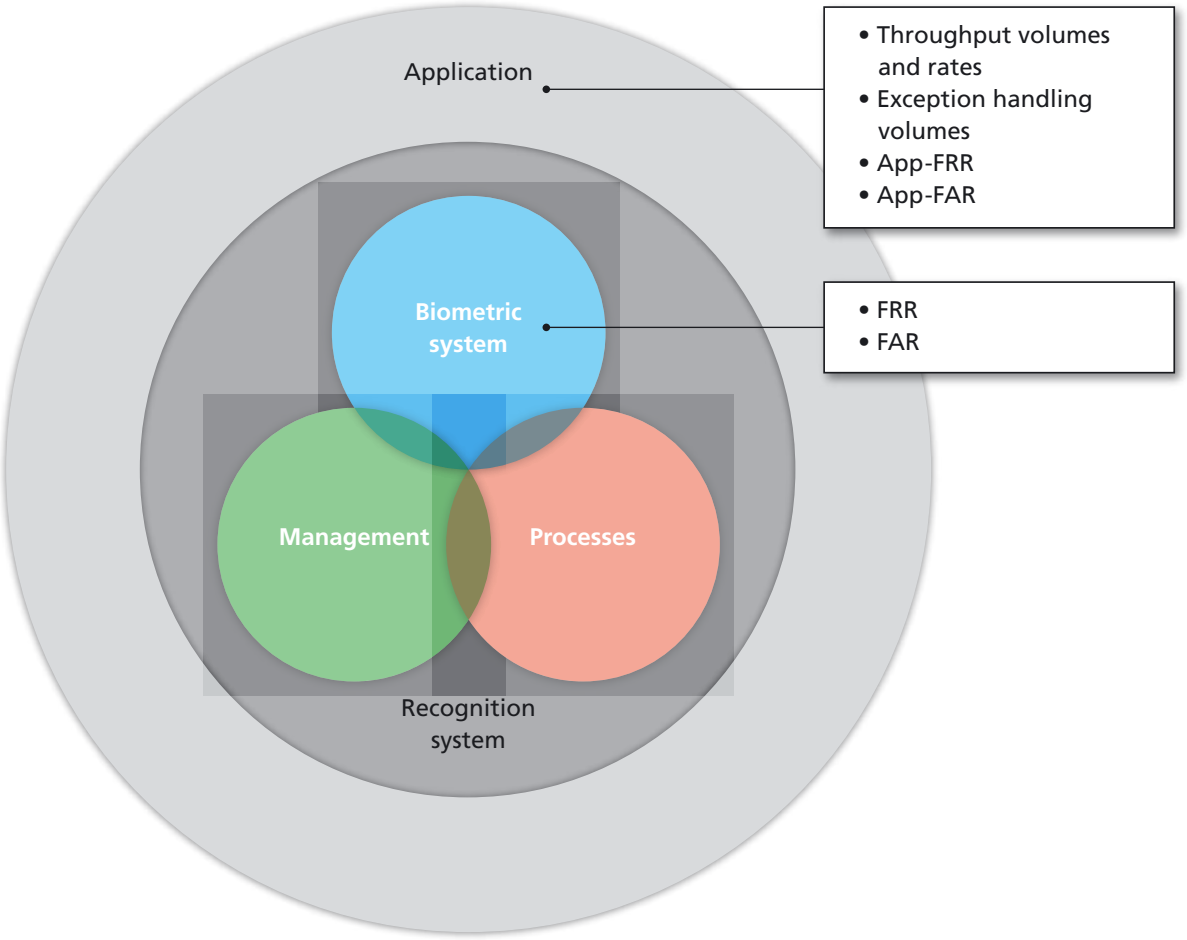
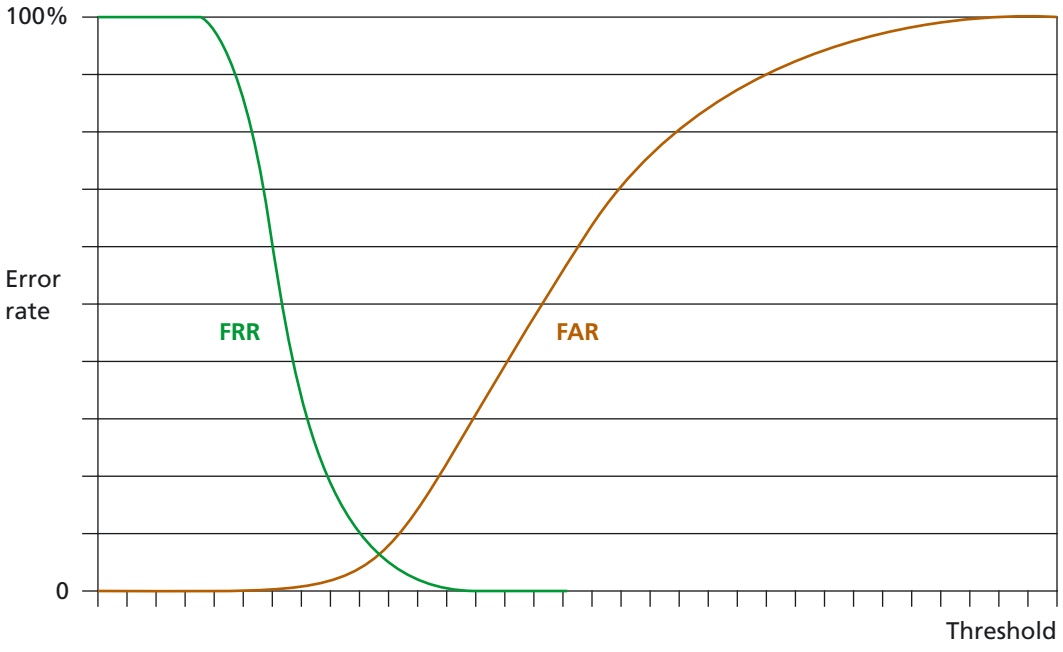


Figure 4 – Example of trade-off between FAR and FRR for different threshold levels



Typically, error rates are quoted for a biometric system and are then difficult to verify when this forms part of an application. Therefore, there is no easy answer to determining the required error rates for a biometric system. The performance parameters that are most important are those that relate to the application, in particular throughput volume and rate, and exception handling volume. Specifying the requirement for these two application performance parameters is fundamental in ensuring the biometric system provides the right solution to the business problem.

From throughput volumes and exception handling volumes, the target application throughput rate and application false rejection rate (App-FRR) can be established.

For example, if an organization has 120 employees who enter the building between the hours of 08:00 and 09:00, and only one data capture station is planned, then the throughput volume would be 120 and the rate for the each biometric capture, claim, recognition process and subject transition would be less than 30 seconds per subject. In practice subjects will actually arrive at different rates and not be spread evenly across the hour. In order to establish how much less than 30 seconds per subject the throughput rate needs to be, an estimate of the peak load and acceptable queue length needs to be taken into account.

If the exception handling process was to comprise one attendant checking a photo ID card used in conjunction with a PIN, then an estimate can be made of how many exception subjects can be handled in the same one hour period. If that assessment was no more than 20 subjects, then a target App-FRR could be determined. This would be less than an implied 16.67% because account has to be taken of all those failing to enrol, and all those with known impairments that cannot use the biometric system, as well as those being rejected by the biometric system. Again subjects will actually arrive at different rates and not be spread evenly across the hour. Therefore, the assessment of being able to handle 20 exceptions in one hour is also likely to be an overestimate.

There is a direct correlation between App-FRR and the biometric system FRR but they will not be the same because the final App-FRR will be influenced by other factors, including the management system and processes in place.

Evaluation of the security risk of incorrect recognition (and thus allowing impostor access) will enable the target application false acceptance rate (App-FAR) to be established. Again there will be a direct correlation between App-FAR and the biometric system FAR but they will not be the same because the final App-FAR will be influenced by other factors including the management system and processes in place.

Note that App-FAR and App-FRR are not widely used terms and therefore discussion with the biometric system supplier is essential to establish a mutual understanding, particularly when agreeing acceptance criteria.

Another significant error rate of a biometric system is the failure to enrol (FTE). FTE is affected by many factors including the subject population, the operational environment and usability. A high FTE is likely to lead to increased exception handling volumes that will have to be accommodated. There is also an impact on the FAR and FRR if the enrolment process controls the quality level of biometric references accepted by the biometric system.

Buyers of a biometric system would naturally wish for ideal performance in all aspects of the system, such as accuracy, usability, accessibility, throughput and security. However, applications using biometric systems are no different from applications using other technologies in that it becomes necessary to make trade-offs between the various competing factors that constitute desirable performance.

Establishment of the required level of performance for an application will provide information that will allow buyers to eliminate biometric systems that will not meet the required level when integrated into the application.

Having identified biometric systems that meet the required level of performance, there will be a need to consider all the remaining performance trade-offs and decide on an optimum balance for the application. Depending on the relative importance of the different factors involved (such as accuracy, usability, accessibility, throughput and security), different choices might be indicated. This judgement is application dependent and it is of paramount importance that those responsible for establishing the required level of performance have a thorough understanding of the application in order to make correct decisions about these trade-offs.

Other performance parameters for the application, such as availability and repair times, will also need to be established but such parameters are considered general to all IT system requirements and so are outside the scope of this PAS.

5.4 Security

5.4.1 The security risks associated with the use of a biometric system for a specific application should be assessed and documented. This should include an assessment of:

a) the risks likely to result from the incorrect recognition of a subject;

b) the risk of integrating the biometric system into other systems; and

c) data protection risks (see **5.9**).

5.4.2 The security requirements for the biometric system should be documented as part of an organization-wide security policy and information security management system.

Security goes beyond the successful recognition of individuals. It is multidimensional and depends upon the nature of the threats as well as the overall system design. Security is affected by:

- fundamental discrimination limits of the technology;
- policies and procedures, which if misstated or misapplied, can completely negate the security; and
- technical vulnerabilities, errors and oversights by users and the sophistication of the attack.

The detailed evaluation of risk, the design of secure systems and the writing of security policies is not covered in this PAS. Instead, further guidance on this and, more generally, information security management systems can be found in BS ISO/IEC 27001 and BS ISO/IEC 27002.

However, it is worth explaining that the level of security offered by a security mechanism is typically expressed in terms of its resistance to attack using internationally recognized attack potential levels of **basic**, **moderate** and **high**.

In the context of recognition, a four-digit access control lock or a four-digit PIN and user ID or smart card provides resistance to an attack potential level **basic**. Further information on attack potentials and comparison between the resistance of password and biometric access control mechanisms is given in Annex B.

Resistance to an attack potential level **basic** is normally considered adequate for access control in a wide range of commercial applications such as those that use four-digit PINs for access control.

Where the application risk assessment has indicated that resistance to a higher attack potential level (i.e. **moderate** or **high**) is needed, specialist security expertise can be sought to advise on suitable solutions for particular requirements. Solutions could include the use of:

- biometric systems that can achieve higher than basic levels of resistance to attack, however, this is likely to limit the choice of technology and could result in poorer usability;
- multi-biometrics (e.g. finger vein combined with fingerprint);
- multi-factor authentication (e.g. biometrics and PIN); and
- supervised recognition.

Annex B provides guidance on specifying values of FAR for biometric recognition systems capable of resisting attack potentials levels of **basic**, **moderate** and **high**. For example, a biometric verification system with a FAR of 1% or lower is deemed to offer adequate resistance to an attack potential level **basic**. As most commercially available biometric verification systems can achieve this figure, for many commercial applications the choice of biometric modality and technology can often be made from other considerations such as FRR, convenience, usability, accessibility and cost.

Specifying a FAR requirement that is more demanding (i.e. lower) than actually needed for the application can be counterproductive because, in seeking to meet an over-specified FAR requirement, the usability and other desirable properties of the system can suffer and the implementation and operating costs are likely to increase. A contributing factor to over-specification can be unfamiliarity with biometric systems generally and the resulting tendency to play safe.

However, in consideration of a casual attempt by an imposter to gain access by achieving a false acceptance, a FAR of 1% (basic) means that 99% of all such attacks will be unsuccessful. In many systems, particularly where failed attackers have a significant chance of being detected and identified, a 99% detection rate is likely to be a highly effective deterrent.

Generally, the biometric system element of an application will probably not be the weak link in security or the point of attack, although there are specific biometric system security considerations and examples of these are described in Annex C.

In some smaller applications, the ability for a biometric system to connect to, or interoperate with, another system will not be a necessary requirement. From the point of view of security and privacy, it might be more acceptable to operate a stand-alone biometric system without the capability of sharing data with other systems. However, often the biometric system will form part of an organization's wider network and processes. For example, it might be integrated with building access control, time and attendance systems, and logical access to a computer network. In such instances, care needs to be taken to ensure integration does not introduce network security weaknesses.

5.5 Usability

5.5.1 A biometric system should be assessed to determine its usability (see Clause **6** on acceptance testing). The assessment should include a determination of whether the biometric system is:

a) intuitive, logical and easy to understand;
b) simple to use with a low physical and cognitive effort;
c) efficient in respect of time taken to accept or reject subjects; and
d) tolerant of error by the subject.

5.5.2 If the subject has to perform a number of actions (e.g. enter an account number, present a card and use a biometric system), the sequence of actions should be logically ordered to help the subject.

5.5.3 Prompts and instructions should be provided by the biometric system:

a) to indicate the location of any user interface;
b) to provide feedback on the success or failure of an action performed on the biometric system by the subject; and
c) where there is a need for an action to be repeated.

The usability of a biometric system is crucial for optimal performance and it is important that detailed attention is given to this aspect.

Specific usability issues for biometric systems are addressed in PD ISO/IEC TR 24714-1. The impact of these issues will vary considerably according to the specific biometric system being used and the application in which it will be deployed.

5.6 Accessibility

5.6.1 A biometric system should be assessed to determine its accessibility (see Clause **6** on acceptance testing). The assessment of accessibility should include a determination of whether the implementation of the biometric system and the application would discriminate against any particular ethnic or social group.

5.6.2 There should be a documented assessment of how a biometric system enables an organization to meet its obligations under the Equality Act 2010 [1], which legislates for equality for several protected characteristics, including disability. This assessment should be reviewed whenever there is a change to the Act.

5.6.3 There should be provision for subjects who cannot use the biometric system or would find it difficult to use, for example:

a) extra assistance;
b) facilities for carers or accompanying guardians;
c) physical privacy; and/or
d) an alternative recognition system (see **5.8** on exception handing).

5.6.4 Prompts should be provided in a combination of audio, visual and tactile forms.

5.6.5 When a biometric system is intended for use by a multicultural subject population, the style of language, metaphors and imagery that are included in any information and training material to be provided in relation to the use of a biometric system should be appropriate for all the respective cultural groups.

5.6.6 Instructions and prompts should be provided in the languages that the subject population would understand.

5.6.7 The location of the data capture station should be clearly indicated to meet the needs of blind or partially sighted people (see **5.7.2** on data capture station).

All recognition systems, whether through smart card, PIN or password, need to cater for impaired populations to some extent. Biometric systems are not exceptional in this regard. So it is important that all reasonable efforts are made to ensure a biometric system is able to be used by as large a proportion of the intended subject population as possible.

No current biometric system can be designed to recognize all individuals. The degree to which a biometric system is accessible will depend on a number of factors, including the nature of the subject population, the usability of the system (see **5.5**) and the physical environment in which it operates.

Some people might have cultural objections to a specific biometric modality. Most cultures accept photographic evidence of identity and therefore might accept a biometric system that incorporates face recognition, but this might not be the case if the culture encourages the wearing of veils or headscarves for certain groups. Individuals in other cultures might have strong objections to touching shared surfaces like fingerprint sensors or hand geometry units, especially if these are not fully visible to the subject. Some biometric systems might perform more poorly when encountering cultural or socially related body ornamentation, such as make-up, tattoos, jewellery, clothing or facial hair, and therefore might not be practical or acceptable.

Some people have registered disabilities that might make biometric recognition difficult. A relatively larger number of people have some other form of impairment that might prevent them using a biometric system as effectively as a subject without such impairment. Some people have a combination of impairments, the cumulative effect of which will amplify the impact of individual impairments. For example, there will be subjects who cannot be enrolled on the system because they lack the required biometric characteristic or the characteristic is so poorly defined or is so unstable as to be unsuitable for use.

Difficulties with accessibility can be long term or temporary and can occur without warning, for example, following the sudden onset of illness such as laryngitis or a sore throat, dental or eye surgery or other physical injury.

In some cases, the problems of accessibility can be mitigated by changes in the design of the environment, for example, by providing height-adjustable data capture devices or optimized lighting conditions. For other degrees of impairment, radical changes in design might be needed.

Whatever strategy is employed in addressing accessibility issues, a biometric system designed with accessibility in mind at an early stage will reduce the risk of challenge under discrimination legislation.

Attention is drawn to the requirements of the Equality Act 2010 [1], which brings together nine different laws that protect people from different types of discrimination. It requires equal treatment in access to employment as well as private and public services, regardless of the protected characteristics of:

- age;
- disability;
- gender reassignment;
- marriage and civil partnership;
- pregnancy and maternity;
- race;
- religion or belief;
- sex; and
- sexual orientation.

Guidance on the Equality Act 2010 [1] is provided by the Equality and Human Rights Commission: http://www.equalityhumanrights.com/advice-and-guidance/new-equality-act-guidance.

5.7 Data capture

5.7.1 Enrolment

5.7.1.1 An enrolment process should be in place and documented, including details of:

a) what credentials to check to establish eligibility to enrol;

b) who is allowed to conduct enrolments in terms of authorization and training;

c) any quality thresholds that have to be met for an enrolment to be deemed successful;

d) how to decide that an eligible subject is unsuitable for enrolment and therefore should use an exception handling process;

e) whether informed consent is required and how to obtain it;

f) training for subjects in using the biometric system; and

g) when re-enrolment takes place and when a subject's enrolled details expire.

5.7.1.2 An assessment should be made as to whether attendants are to be present at enrolment. If attendants are present, they should be specifically trained in the process and the data capture station should provide feedback to them as to the success or failure of enrolments.

5.7.1.3 Subjects should be informed, as a minimum and as part of the enrolment process, about the reasons for the use of a biometric system, about how accessibility has been built into the system (including reference to exception handling) and of the privacy notice (see **5.9.4**).

5.7.1.4 Subjects should be trained in the use of the biometric system during enrolment and given the opportunity to practice using the system in order to increase familiarity.

Enrolment is generally defined as the process of collecting one or more biometric samples from an individual, and the subsequent creation of a biometric reference against which future comparisons will be made to recognize the individual. The performance and usability of a biometric system is critically dependant on the quality of the biometric enrolment data. Poor quality enrolments might require comparison thresholds to be set in ways that weaken the security of the application to mitigate the poor usability of the biometric system by the subject.

There are a number of factors that affect the quality of the biometric sample captured during enrolment, these include:

- enrolment procedures;
- training of enrolment attendants;
- design of the data capture station (see **5.7.2**); and
- environmental factors at the data capture station (see **5.7.3**).

Well trained enrolment attendants can often provide valuable assistance to enrolees who are experiencing difficulties, although this can be subject to limitations where, for example, the operational policy prohibits attendants from physically touching enrolees to help position them correctly. The attendants' experience can reduce the variability of quality of the biometric reference introduced by unhelpful aspects of human behaviour including the wrong pose, an unwanted facial expression, dry skin or a medical condition.

The use of trusted enrolment attendants might also be an effective safeguard against malevolent enrolees who might seek to subvert the enrolment process, e.g. through the attempted use of an artefact.

The presence of well-trained attendants at enrolments has been shown to significantly improve the quality of biometric references. The quality of biometric references in turn has a significant effect on the biometric system FAR and FRR.

A subject's entitlement to be enrolled in a biometric system can be established as part of the enrolment process. For example, their identity might be confirmed through the registration of non-biometric personal data whose authenticity and integrity can be checked by trusted enrolment attendants ("identity proofing").

The enrolment process is likely to be the first time that the subject comes in contact with the biometric system equipment. The enrolment procedure needs to inform and relax the subject and is likely to include:

- direct face-to-face support;
- written material (provided in an inclusive and comprehensible manner) in the form of posters and information leaflets; and
- multimedia demonstrations.

As with the introduction of any new technology, subject familiarity and past experiences of biometric systems will have a considerable effect upon acceptance and subsequent successful use. So, it is important to train the subject in the use of the system early on and to ensure the training is a positive experience. Also, providing an opportunity to practice using the system will help habituation, which can improve both the quality of biometric samples taken and the throughput of the system.

Even simple issues can cause additional problems, which could be avoided by planning ahead and training. For example, if a subject and attendant sit facing each other, they need to establish a mutually agreed view of "left" and "right" if this is significant in the enrolment process.

In some cases the subject could be unaware of the fact that a biometric enrolment is taking place, for example, when submitting a photograph for an application where the photograph is used to enrol the subject in the system. In such circumstances, it is important that a subject is aware of what data are being recorded and how the data are going to be used.

One systematic source of variability of biometric performance is the changes that occur over time in a subject's biometric characteristics caused by biological ageing or behavioural changes. This can give rise to an increase of false rejections. A subject's capability to use a biometric system can also degrade with illness or injury. Therefore, it might be necessary for re-enrolment to be carried out at a fixed interval of time or in response to reductions in matching performance recorded by the system over time.

5.7.2 Data capture station

5.7.2.1 A data capture station should be designed to be usable (see **5.5**) and accessible (see **5.6**) for both subjects and attendants.

5.7.2.2 The configuration of a data capture device should be determined through an assessment of:

a) how the subject will interact with the device and any attendants in terms of both physical and psychological comfort; and

b) how easy it is to collect a biometric characteristic with the best achievable quality.

5.7.2.3 The design of a data capture station should take account of whether the station is attended or unattended.

5.7.2.4 A data capture station should be designed and located to prevent individuals not involved in data capture from interfering with the process of data capture.

5.7.2.5 An assessment of whether attendants and personal assistants are allowed to assist subjects during data capture should be conducted and, if so, the design of any designated data capture station should be such that it accommodates this assistance.

5.7.2.6 A data capture station should be designed to accommodate variations in the height and reach of the subject population.

5.7.2.7 Feedback should be given to the subject to assist with the correct presentation of their biometric characteristic.

5.7.2.8 If a subject is required to wear personal protective equipment (PPE) when using a biometric system, the system should be one that allows the subject to present a biometric characteristic without having to remove the PPE.

The ergonomic design of a data capture station has a very strong correlation with the quality of captured biometric characteristic (for both enrolment and recognition) and for the satisfaction felt by the subject.

The design of a data capture station needs to take account of the target subject population, in particular whether there will be a need to accommodate subjects who might have difficulties with enrolment or recognition because of disability or other physical or cognitive problems. Examples include wheelchair users, arthritis sufferers, those with auditory or visual impairments and those with medical conditions that render them unable to control their limbs, head or eyes.

Designing data capture stations to deal with these conditions can be extremely challenging. Conditions will militate against the choice of a specific biometric modality. Flexibility in adjustment in height and angle of data capture devices or a choice of alternative data capture devices can help to improve accessibility for a wider range of enrolees with disabilities and other medical conditions. Therefore the position and orientation of a data capture device is also an important consideration.

Feedback to assist subjects in presenting their biometric characteristics correctly to the data capture device is helpful, for example, feedback on where to place a finger on a fingerprint reader or where to stand and look for a facial recognition or iris systems. This feedback could be provided either automatically by the equipment or manually by an attendant (if present) and is best given at the point of use.

Appropriate designs of a data capture station for enrolment or recognition can take the form of, for example, a desktop workstation, an "across the counter" setup, a "pod" configuration, a kiosk or a mobile kit. Selection of the configuration will depend on a number of factors, including environmental, space and cost considerations.

Protective clothing can present problems for data capture devices depending on the biometric modality used. For example, if protective gloves have to be worn, fingerprint recognition would be unlikely to be suitable. Other examples of possible problem clothing types are hard hats, protective glasses, goggles and welders' masks, face masks that cover the mouth and nose, and heavy boots or knee protectors that could modify a subject's posture.

5.7.3 Environment

5.7.3.1 A data capture device should be maintained in the environmental conditions specified by the manufacturer of the device as optimum for the performance of the biometric system otherwise performance could be compromised.

5.7.3.2 An assessment should be conducted to identify whether there is a need to house the data capture device in an enclosure (such as in a separate room, in an enclosed booth or with a simple guard covering the device) to ensure the optimum performance of the device is maintained.

5.7.3.3 Where a data capture device is monitored in direct line of sight or using CCTV to enable assistance to be given or to spot and record malevolent behaviour, the device should be located in such a way that there is an unobstructed view of the interaction between the subject and the device.

5.7.3.4 Lighting in the vicinity of a data capture device should be assessed to determine if it maintains the level of security required for the vicinity whilst minimizing possible interference to the device by excessive or uneven illumination.

5.7.3.5 Ambient noise in the vicinity of a data capture station should be assessed to determine whether the noise could interfere with audible instructions given to subjects or could interfere with the acquisition of a biometric sample, e.g. for voice recognition.

All biometric systems are subject to variability in performance due to a range of environmental factors, including those associated with the built environment, such as lighting, temperature, audible noise and electrical noise.

It is particularly important to ensure good environmental conditions for enrolment because poor conditions will usually result in the creation of low quality biometric references, which will lead to poor performance through increased biometric recognition error rates. The failure to enrol (FTE) rate and application false rejection rate (App-FRR) are likely to be substantially higher than those that can be achieved under good environmental conditions.

Problems can be created by extremes of temperature and humidity, contamination from dust or chemicals, the need for protective clothing and protection against vandalism, levels of artificial or natural illumination, the position and orientation of the biometric device and the presence of other fixtures and fittings in the vicinity. The extent to which these have an impact on the biometric system performance varies according to the biometric modality.

Climatic extremes, in particular extremes of temperature or humidity, can present problems to sensitive data capture devices and hinder the capture of good quality biometric data. For example, extremely dry environments might not allow optimal capture for fingerprints and in outdoor locations exposure to fog, rain or snow and ice or condensation on a sensor such as a camera lens can affect data capture.

Subjects can also be affected by climatic conditions in a way that impacts upon biometric system performance. They might have to remove gloves, hats, scarves or sunglasses. Extremes of temperature can cause fingerprints to be more dry or moist depending on the environment. High temperatures could cause the subject to sweat excessively impeding the capture of the biometric data.

The ambient environment can also have an adverse effect. High levels of ambient noise from people, machinery, public address systems or traffic might prevent biometric data from being collected or recognized where the biometric modality is sensitive to noise levels (e.g. when voice recognition is the biometric modality). Such noise interference can also prevent users and subjects from hearing spoken instructions, which can be especially problematic for blind or partially sighted subjects who rely on these instructions.

Contamination from dust or chemicals is another environmental factor to consider (e.g. in engineering or industrial locations or in locations where food is prepared and there are high levels of oil particles from frying food). Under such conditions, it can require unusually high maintenance to keep a data capture device clean and to prevent corrosion, so it is a good idea to keep devices in an enclosure that is protected from the working environment.

A data capture device in an external location or internal public space can be subject to additional challenges, such as vandalism including attack with a heavy or sharp object or by spray-painting. The use of CCTV or the presence of attendants could act as a deterrent to such activities.

In many public areas it could also be useful to provide booths or kiosks where the environment can be controlled to enable the performance requirements of a data capture device to be achieved.

Further information on the environmental sensitivities of biometric modalities can be found in PD ISO/IEC TR 24714-1.

5.8 Exception handling

5.8.1 An exception handling process should be in place to provide an alternative means of recognition to accommodate:

a) occurrences of false rejection; and

b) a subject who is unable to use the biometric system as a result of a particular disability or impairment.

5.8.2 The exception handling process should be capable of handling the volume and nature of exceptions likely to be encountered among the population of subjects (see **5.3.1**).

5.8.3 The exception handling process should be reviewed after a specified period of time and in the light of operational experience with the aim of improving the process to address issues where they are identified.

It is important to recognize that an exception handling process is a potential security vulnerability because many exception handing processes can offer less security than the biometric system.

An assessment of the likely exception handling volume, perhaps by reference to other similar biometric systems that have already been deployed, is an essential part of planning for the implementation of a biometric system. The exception handling volume can even amount up to 5% to 10% of the expected total number of subjects using a biometric system.

The exception handling process can consist of:

- another instance of the same biometric modality (e.g. a different finger on a fingerprint system);
- an alternative modality (e.g. iris image modality instead of a fingerprint modality);
- some other form of machine-readable identification (e.g. smart card and PIN); and/or
- another individual, normally a member of staff, identifying the individual using comparison of his/her

appearance or signature to the corresponding image on an identity document.

For example, in the case of physical access control where biometric recognition might generally be controlling a turnstile or door, the exception handling process could be an attended entry facility for wheelchair access.

It is important that any exception handling process is designed to accommodate the number of exceptions that an application is expected to encounter. The exception handling volume can be estimated by assessing the expected application false rejection rate (App-FRR) against the expected throughput volume.

Exception handling processes will need to be designed and implemented with attention to security requirements. If the exception handling system security is weaker than the primary recognition system, forcing an exception could be used to exploit this security weakness.

5.9 Privacy and data protection

5.9.1 There should be a documented assessment of how a biometric system enables an organization to meet its obligations under the Data Protection Act 1998 [2], which legislates for the handling of personal data. This assessment should be reviewed whenever there is a change to the Act.

5.9.2 A policy relating to the protection of personal data should be documented and should include:

a) a requirement that biometric data are considered as personal data and that mechanisms to secure that data are provided;
b) how any biometric data are to be secured;
c) who is responsible for the security of retained personal data;
d) how long any biometric data are to be held;
e) how any biometric data which are no longer required are to be deleted;
f) which authorities can be provided with biometric and/or associated data;
g) the conditions and limitations under which any biometric and/or associated data can be provided;
h) what authorizations are required to be in place to provide biometric and/or associated data to other authorities;
i) who should have specified access rights to personal data (including rights to modify and delete), under what circumstances and under what supervision;
j) what personal data can be accessed, modified and deleted;
k) what notification will be given to the data subject; and
l) the process for investigating and redressing any complaint of retention contrary to the policy.

5.9.3 The personal data to be collected by a biometric system should be identified and its collection justified.

5.9.4 A privacy notice should be made available to enrolees to inform them, as a minimum, about which organization is collecting the data, what data the organization will be collecting and what the organization intends to do with the data (including any organizations the data will be shared with).

5.9.5 Assurances about the measures in place to protect stored biometric and other personal data from loss or unauthorized disclosure should be available to subjects.

5.9.6 A method for verifying the accuracy of the collected personal data and providing support for the correction of any identified errors should be in place.

5.9.7 All access and modifications to personal data should be documented.

5.9.8 A senior person who is accountable for the purpose and manner in which personal data are collected, processed, stored and disposed of should be appointed.

5.9.9 All staff who act as handlers of personal data should be informed and trained in their responsibilities in the management of personal data.

Data protection is an important consideration in planning for the implementation of a biometric system and its associated application.

Attention is drawn to the Data Protection Act 1998 [2], which legislates for the protection of personal data. Biometric data is considered as personal data in accordance with the Data Protection Act 1998 [2] and the eight principles of data protection given in the Act apply to biometric data as they do other types of personal data. A summary of the eight principles of data protection is given in Annex D.

The Information Commissioner's Office (ICO) has developed an approach whereby privacy and data protection compliance is designed into systems holding personal data right from the start of a project, rather than being added on afterwards. It is called *Privacy by Design* [3] and advocates that organizations should address privacy concerns throughout the lifecycle of the system. Performing privacy impact assessments, managing privacy risks and promoting greater transparency are all aspects of privacy by design. Detailed guidance is given on the ICO website: http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/privacy_by_design.aspx.

A core set of identity data often centres on personal data such as name, birth date, and address. The introduction of a biometric system might reduce the amount of additional personal data that has to be collected and stored purely for identification purposes. However, many people still have concerns about the privacy of their biometric and associated data, specifically that the data might be used for purposes other than those that have been declared or that the data might be shared with organizations other than those that have been declared. This could be perceived as a heightened risk for biometric data because biometric data could provide a means of linking non-biometric data about one individual stored on different systems. Therefore, privacy safeguards can be a critical acceptance factor for individuals who are to use biometric systems.

Experience shows that privacy concerns can be minimized by transparency, particularly in the publication of advance information about the justification for the biometric system and the ways in which the biometric data will be used, shared and processed. The provision of a privacy notice can provide confidence to subjects about the use of their data. The ICO has produced a code of practice for the provision of privacy notices and this available from their website: http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/privacy_notices.aspx [4].

6 Acceptance testing a biometric system

6.1 Acceptance of the biometric system should be based on tests that demonstrate conformance to the performance requirements specified during procurement, including:

a) throughput volumes and rates;

b) exception handling volumes;

c) application FRR (App-FRR) and application FAR (App-FAR);

d) usability in terms of the efficiency of the system, its effectiveness and the satisfaction of users (such as subjects, attendants and supervisors); and

e) accessibility.

6.2 The number of subjects selected to test the performance parameters in **6.1** should be representative of the expected type and volume of subjects and attendants.

6.3 All biometric system settings including threshold settings that are set during acceptance testing should be documented and subsequently controlled during operation (see **7.3** on change management).

6.4 If the biometric system threshold settings are altered at any stage during or after acceptance testing, any acceptance testing related to the changed settings should be repeated.

6.5 All results generated from acceptance testing should be documented.

Throughput volumes, exception handling volumes and App-FRR testing are all interdependent. The App-FRR will be the main driver in the generation of exceptions. Increased volumes of exception handling will reduce the throughput of the application. However, altering the biometric system threshold settings to reduce the number of false rejections might not be the solution to an unacceptable App-FRR as this might not meet the security requirements for the application. The most likely reasons for a higher than anticipated App-FRR will be:

- subject unfamiliarity with the biometric system;
- poor biometric reference resulting from poor enrolment;
- inadequate training of attendants; and
- poor design of the data capture station, in particular instructions and prompts (including signage).

Impostor testing can also form part of the acceptance testing. This will not directly represent the FAR of the biometric system or the App-FAR. However, by attempting impostor testing, an assessment can be made of the application security with all of the security procedures in place. In particular, the exception handling process and fallback arrangements can be exercised to assess if unacceptable security weaknesses have been introduced into the application.

Usability and accessibility have to be tested to quantify the subjective nature of subject perceptions. Surveys of these perceptions can be compiled to elicit issues and provide quantifiable measures. Such surveys can be anonymous. Note, however, that personal data might need to be collected to enable the assessment of trends or groupings within the results. Such data might include:

- age;
- gender;
- ethnicity;
- left or right handedness;
- known impairments; and
- height.

Quantification of subject perceptions can be arranged in steps from "strongly agree" to "strongly disagree". It is preferable to ensure the number of steps force a decision rather than allowing an easy default to "neither agree nor disagree".

Subject surveys can also be supplemented by in depth subject interviews and behavioural observations conducted by trained independent observers.

Usability and accessibility results can be used for acceptance testing as well as for corrective action or improvement planning.

Some acceptance testing can require an extended period of time for completion, so system acceptance might not be signed off until well after operational use has commenced. For example, biometric system performance is likely to improve as subject familiarity increases. Similarly, as familiarity increases the volume of exception handling might decrease. This can provide the opportunity to review the biometric system threshold settings as part of change management procedures (see **7.3**), noting that biometric system performance would need to be retested if thresholds are changed.

Further information on biometric performance testing and reporting can be found in BS ISO/IEC 19795.

7 Operating a biometric system

7.1 Legislation

7.1.1 Legislation applicable to the use of a biometric system should be identified and a review should be conducted to determine how the legislation applies to the operational processes associated with a biometric system.

7.1.2 The operational processes associated with the biometric system should be reviewed whenever there is a change to applicable legislation to determine whether any changes to operational process are required.

This PAS draws attention to the Equality Act 2010 [1] and the Data Protection Act 1998 [2]. However, it does not aim to provide an exhaustive list of legislation that is applicable to the use of biometric systems and an organization operating a biometric system is advised to make necessary efforts to identify legislation that applies to their particular use of a system.

7.2 Maintenance

7.2.1 A biometric system should provide alerts in the event of malfunctions or degradation in performance so that maintenance procedures can be performed.

7.2.2 A biometric system that has undergone maintenance should be tested to determine that it is still operating as expected. A description of the type of testing to conduct after each maintenance task should be documented.

7.2.3 A data capture device should be cleaned in accordance with the manufacturer's instructions to avoid contaminants such as moisture, dust or debris from affecting the performance of a biometric system.

Some data capture devices, particularly those that come in contact with people during use, will need regular maintenance. Manufacturers generally specify details of their equipment's maintenance requirements, including which types of cleaning products to use. It is important that maintenance and cleaning personnel be instructed in these requirements.

7.3 Change management

7.3.1 Changes to the settings of a biometric system should be made in accordance with a documented procedure, which should include a risk assessment and an auditable approval of the new settings.

7.3.2 Following any changes to the settings of the biometric system, testing should be conducted to verify that the performance conforms to specified criteria. Such tests can be a repeat of those performed during acceptance testing (see Clause **6**).

Biometric system thresholds that have an impact on FAR and FRR are set at the time of installation and are only changed following a documented procedure. Where thresholds are relaxed in an attempt to lower the number of false rejections of legitimately enrolled subjects, without the support of a structured risk assessment and testing, security breaches can occur that have not been anticipated. Therefore, it is essential that a thorough risk assessment is first completed before making any changes in the biometric system threshold to minimize the risk that the security of the system is compromised if the FAR is allowed to increase. The impact of a relaxation in threshold setting on the FAR is shown in Figure 4.

It is useful to consider developing a policy for equipment replacement as part of the change management process. This might involve a change of supplier, equipment or software rather than just a like-for-like swap. The use of equipment that conforms to international standards, such as those produced by the International Organization for Standardization (ISO), could simplify the replacement process and ensure long-term viability of the biometric system.

7.4 Management information system data

A biometric system should make provision for the collection of management information system data, to allow the monitoring and analysis of trends in performance.

Management information system data could include data capture times, data quality and system match/non match decisions. Trend analysis of such statistics could help in making decisions on, for example, equipment replacement or alterations in maintenance schedules.

7.5 Fallback arrangements

7.5.1 Fallback arrangements should be in place in order that an application can continue in the event of a biometric system failure or while elements of a biometric system are under repair or adjustment.

7.5.2 Fallback arrangements should conform to previously defined security requirements to ensure that system security is not compromised during fallback operation.

7.5.3 Fallback arrangements should be tested to validate their effectiveness.

Fallback arrangements are specific to the biometric system and would form part of an organization's overall business continuity plan. Further guidance on business continuity management is given in BS 25999.

Annex A (informative)
Basic principles of a biometric system

A.1 General

A biometric characteristic is a physical or behavioural feature or attribute that can be observed and used for automated recognition. It does not directly reveal "identity", but can link to records that have established identity by non-biometric means. All biometric characteristics contain both physical and behavioural elements.

A sensor converts the biometric characteristic into a pattern of numbers (perhaps microphone voltage levels or pixel values) that can be transformed through some indirect mathematical process into measures that are distinctive to an individual and reproducible over time.

The basic principle of a biometric system is that certain physical and behavioural characteristics are distinctive. Therefore, the enrolled attribute of a subject is more likely to match that subject than any other subject the system is likely to encounter. Some, but not all, biometric characteristics can even individuate a person from a large population. However, it is not necessary for a biometric characteristic to be capable of individuation for it to be useful in access control or other simple applications (such as time and attendance systems).

It is very important to understand that, on its own, a biometric characteristic such as a fingerprint does not identify a person in the usual sense. When a biometric characteristic is acquired or observed, it can only ever be used to search for a match with another record already stored in some form. In the simplest application, the fingerprint might be compared only with a record held on a plastic card which is carried by the person concerned. In that case, a successful match with that record conveys no information other than confirmation that the card holder is present in person. This matching process might be carried out locally inside the machine and without any communication to a centralized system or centralized store of data.

Similarly, if a biometric characteristic alone, without any additional supporting data, is acquired following payment of an entry fee to a theme park and then used for admission to the various rides within the park, the only information conveyed is that the possessor of the biometric characteristic has paid their entry fee. Such a system is sometimes referred to as an example of "anonymous biometrics".

A.2 What is a biometric system?

A biometric system is essentially a recognition system that operates by acquiring biometric data from an individual, extracting a feature set from the acquired data, and comparing this feature set against the biometric reference set in a database, on a card, etc.

Biometric systems using one biometric modality are deployed in many types of application contexts, such as airports and physical and logical access control. It has been suggested since the 1970s that by combining more than one modality (multimodal operation), enhanced performance reliability and even increased subject acceptance could be achieved, but there is as yet insufficient experience of the use of large-scale multimodal operation to corroborate this theory. Combining less reliable technologies in sequence could strengthen the overall biometric system performance and combining them in parallel could increase the flexibility of the biometric system by providing alternative modes for the recognition process, but both approaches could increase error rates, costs and data collection times.

Biometric characteristics are said to be "distinctive". The distinctiveness of a biometric characteristic varies by the technique used to measure it and the process by which two similar biometric references are declared as matching. Also, every biometric feature sampling process results in the creation of a slightly different biometric reference, so the matching process has to be tolerant of such variations.

Biometric characteristics can be considered as a bridge between an identity record and the individual to which this record refers. In this way biometric recognition establishes a "trusted" method to strongly link the stored identity with the physical person it represents. This type of biometric recognition is desirable and necessary on many occasions, in contrast with the use of "anonymous biometrics" (see **A.1**).

A.3 Biometric recognition

Biometric recognition works in the following four stages.

a) Enrolment

An individual is enrolled, i.e. a biometric reference is created associating the identifying features with the individual. For example, an iris scan is performed and the resulting reference is labelled, typically with a name, although in the case of an anonymous system, a label might be used that has no meaning or linkage outside the system.

b) Storage

The biometric data acquired during the enrolment are stored as a biometric reference, in general through transformation by proprietary software, to allow for ease of comparison in subsequent use. Two common options for the storage of biometric references include storage on a central database or decentralized storage, for example, on smart cards.

c) Acquisition

When recognition is required at some time after enrolment, a new sample of the biometric characteristic is acquired, for example, a new iris scan performed.

d) Matching

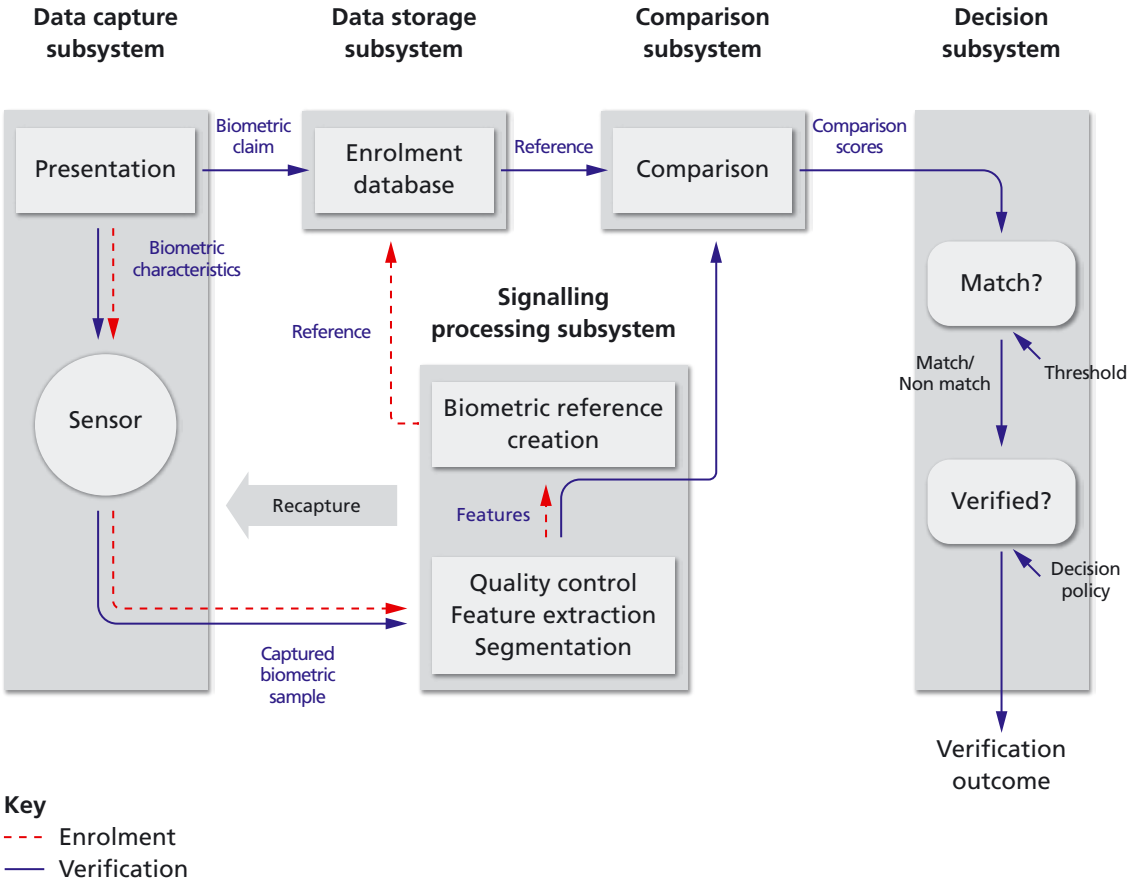
The newly acquired sample is processed and compared with the reference stored for the individual at the time of enrolment. If they are sufficiently similar a match is declared through a decision process and the individual is deemed to be recognized.

Requiring that the sample and enrolment reference be "sufficiently similar" means that biometric recognition is probabilistic and subject to statistical constraints. Variations in conditions between enrolment and subsequent sample acquisition as well as bodily changes (temporary or permanent) mean that there is rarely a perfect match between an acquired (and processed) sample and the enrolment reference. Verification using biometric recognition is markedly different from providing an identity using a password or a PIN. A subject-supplied PIN or password either is or is not exactly the same as the one that has been stored. The smallest deviation is a reason for a refusal to verify an identity. For a biometric characteristic, there is no clear line between a match and a non match. Whether a match exists depends therefore not only on comparison of the sample and reference data sets, but also on the permitted margin of error. As a consequence of the variability in biometric characteristics, there is always a potential for failure to prove a match.

The biometric data themselves (the samples acquired either at the time of enrolment or at verification), need not actually be stored in the biometric system. Iris images, fingerprints and face images are converted into abstract numerical data sets via mathematical algorithms and stored as biometric references. The use of mathematical algorithms is intended to permit reliable comparison of biometric samples even over changes in minor detail upon each re-sampling. Whilst the algorithms are different for each technology and even between suppliers of each technology, this procedure is usually non-reversible, i.e. it is not possible to recreate the initial image from a biometric reference.

Figure A.1 shows the information flow within a general biometric system consisting of data capture, signal processing, storage, comparison and decision subsystems. This figure illustrates both enrolment, and the operation of recognition systems. It is derived from BS ISO/IEC 19794-1:2006.

Figure A.1 – Components of a biometric system



Annex B (informative)
Relationship between security and false acceptance rates

The false acceptance rate (FAR) is one of the performance parameters that has an impact on the security of a biometric system and might need to be considered when deciding whether or not to use a recognition system that incorporates biometric recognition.

The *Common Criteria for Information Technology Security Evaluation* (CC) [5] uses the concept of "attack potential" as a measure of the effort to be expended in attacking an IT system, expressed in terms of an attacker's expertise, resources and motivation. CC is identical to BS ISO/IEC 15408.

CC defines three levels of attack potential: **basic**, **moderate** and **high**. The associated *Common Methodology for Information Technology Security Evaluation* (CEM) [6] provides a rationale for assessing the strength of a statistically or probabilistically based authentication mechanism such as a PIN or password. CEM is identical to BS ISO/IEC 18045. A CEM analysis concludes that a four-digit PIN is capable of resisting an attack potential of level **basic**.

Biometric authentication is also subject to statistical and probabilistic considerations and the *Biometric Evaluation Methodology* (BEM) [7] has adapted the CEM model to address biometric authentication in a similar threat environment to that for the PIN assessment. BEM suggests false acceptance rate (FAR) values for biometric authentication that are needed to provide the strength of mechanism capable of resisting the CC attack potential levels as shown in Table B.1.

Table B.1 – Resistance to attack potential related to FAR

Resistance to attack potential	FAR
Basic	<1 in 100 (1%)
Moderate	<1 in 10 000 (0.01%)
High	<1 in 1 000 000 (0.000 1%)

It is important to note that the FAR figures in Table B.1 relate to the biometric system and not to the application as a whole. Other factors can affect the application false acceptance rate (App-FAR) including procedural security weakness and the security of the exception handling process (see **5.8**) and fallback arrangements (see **7.5**).

Note that, whilst this annex focuses on the affect of FAR on the security of a biometric system, other factors can also compromise the system's security, such as poorly designed physical controls, databases and information management systems.

Annex C (informative)
Examples of security risks and countermeasures associated with a biometric system

C.1 Spoofing

Spoofing is fooling a biometric system by means of an artefact bearing a copy of the biometric features of an enrolled subject. It is a concern because spoofing directly undermines the principal strength of biometric authentication, namely that biometrics directly binds the individual to the authentication process in a way that other forms of authentication cannot do.

The source images for biometrics are not generally secret. People carry and leave latent images of their fingerprints, faces can be easily photographed, voices recorded and so on.

A liveness check is one countermeasure to spoofing. Liveness checks detect physical properties of the live biometric, e.g. thermal measurement or the presence of a natural spontaneous signal such as pulse.

Liveness is generally used in conjunction with other measures, such as supervised operation and challenge/response exchanges, for greater security.

C.2 Capture replay

If an impostor can capture the electrical signals containing the biometric features of an authorized user, it might be possible to replay them later to allow the impostor to impersonate the authorized user. Protection can be provided by:

- tamper resistant systems or armoured cables;
- supervised operation;
- encryption (using unique session keys);
- time stamping of the signals; and
- challenge/response.

Challenge/response is directed principally at countering capture/replay attacks, but it might also have a useful role as a form of liveness check in some cases. By issuing a challenge requiring one of a variety of different responses, it makes it harder for an impostor to simply replay a recorded signal.

C.3 Biometric reference integrity and confidentiality

Biometric reference integrity and confidentiality are often confused. In fact, they serve different purposes. Biometric reference integrity protection serves to guard against a fake biometric reference being introduced or a genuine one being modified. Biometric reference confidentiality guards biometric data from being disclosed to others – in other words addressing the data privacy issue. Both biometric reference integrity and confidentiality can be protected using cryptographic techniques, applied to the biometric database and communications between systems.

Annex D (informative) Data protection principles

The Data Protection Act 1998 [2] lists the following eight data protection principles.

1) Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:
   a) at least one of the conditions in Schedule 2 of the Data Protection Act 1998 [2] is met; and
   b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 of the Data Protection Act 1998 [2] is also met.

2) Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3) Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4) Personal data shall be accurate and, where necessary, kept up to date.

5) Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6) Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 1998 [2].

7) Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8) Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Bibliography

Standards publications

For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

BS 25999 (all parts), *Business continuity management*

BS ISO/IEC 15408 (all parts), *Information technology – Security techniques – Evaluation criteria for IT Security*

BS ISO/IEC 18045, *Information technology – Security techniques – Methodology for IT security evaluation*

BS ISO/IEC 19794-1:2006, *Information technology – Biometric data interchange formats – Framework*

BS ISO/IEC 19795, *Information technology – Biometric performance testing and reporting*

BS ISO/IEC 27001, *Information technology – Security techniques – Information security management systems – Requirements*

BS ISO/IEC 27002, *Information technology – Security techniques – Code of practice for information security management*

PD ISO/IEC TR 24714-1:2008, *Information technology – Biometrics – Jurisdictional and societal considerations for commercial applications – Part 1: General applications*

Other publications

[1] GREAT BRITAIN. Equality Act 2010. London: The Stationery Office.

[2] GREAT BRITAIN. Data Protection Act 1998. London: The Stationery Office.

[3] INFORMATION COMMISSIONER'S OFFICE (ICO). *Privacy by Design*. Available from: http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/privacy_by_design.aspx

[4] INFORMATION COMMISSIONER'S OFFICE (ICO). *Privacy Notices – Code of Practice*. December 2010. Available from: http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/privacy_notices.aspx

[5] COMMON CRITERIA. *Common Criteria for Information Technology Security Evaluation*. July 2009. Available from: http://www.oc.ccn.cni.es/xml

[6] COMMON CRITERIA. *Common Methodology for Information Technology Security Evaluation*. July 2009. Available from: http://www.oc.ccn.cni.es/xml

[7] BIOMETRICS WORKING GROUP. *Biometric Evaluation Methodology (BEM) – Common Criteria – Common Methodology for Information Technology Security Evaluation*. August 2002. Available from: http://www.cesg.gov.uk/policy_technologies/biometrics/media/bem_10.pdf

Further reading

BS ISO/IEC 2382-1, *Information technology – Vocabulary – Part 1: Fundamental terms*

BS ISO/IEC 15944-1, *Information technology – Business agreement semantic descriptive techniques – Part 1: Operational aspects of Open-edi for implementation*

BS ISO/IEC 19794 (all parts), *Information technology – Biometric data interchange formats*

BS ISO/IEC 24761, *Information technology – Security techniques – Authentication context for biometrics*

BS ISO/IEC 29109, *Information technology – Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794*

BS ISO/IEC 29794 (all parts), *Information technology – Biometric sample quality*

ISO 19092, *Financial services – Biometrics – Security framework*

ISO/IEC 24760, *Information technology – Security techniques – A framework for identity management* [1)]

ISO/IEC 29100, *Information technology – Security techniques – Privacy framework* [1)]

ISO/IEC 29120 (all parts), *Information technology – Machine readable test data for biometric testing and reporting* [1)]

ISO/IEC 29144, *The role of biometrics in identity management* [1)]

ISO/IEC TR 29194, *Guidance on the inclusive design and operation of biometric systems* [1)]

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). *Electronic Authentication Guideline*. NIST Special Publication 800-63, Version 1.0.2, April 2006. Available from: http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf

PD ISO/IEC Guide 71, *Guidelines for standards developers to address the needs of older persons and persons with disabilities*

Useful websites

BSI
http://www.bsigroup.com/biometrics

Biometrics Working Group (BWG)
http://www.cesg.gov.uk/policy_technologies/biometrics

The Information Commissioner's Office
http://www.ico.gov.uk

[1)] In preparation.

British Standards Institution (BSI)

BSI is the independent national body responsible for preparing British Standards and other standards-related publications, information and services.

It presents the UK view on standards in Europe and at the international level.

It is incorporated by Royal Charter.

Revisions

British Standards are updated by amendment or revision. Users of British Standards should make sure that they possess the latest amendments or editions.

It is the constant aim of BSI to improve the quality of our products and services. We would be grateful if anyone finding an inaccuracy or ambiguity while using this PAS would inform the Knowledge Centre.

Tel: +44 (0)20 8996 7004 Fax: +44 (0)20 8996 7005
Email: knowledgecentre@bsigroup.com

BSI offers Members an individual updating service called PLUS which ensures that subscribers automatically receive the latest editions of standards.

Tel: +44 (0)20 8996 7669 Fax: +44 (0)20 8996 7001
Email: plus@bsigroup.com

Buying standards

You may buy PDF and hard copy versions of standards directly using a credit card from the BSI Shop on the website **www.bsigroup.com/shop**. In addition all orders for BSI, international and foreign standards publications can be addressed to BSI Customer Services.

Tel: +44 (0)20 8996 9001 Fax: +44 (0)20 8996 7001
Email: orders@bsigroup.com

In response to orders for international standards, it is BSI policy to supply the BSI implementation of those that have been published as British Standards, unless otherwise requested.

Information on standards

BSI provides a wide range of information on national, European and international standards through its Knowledge Centre.

Tel: +44 (0)20 8996 7004 Fax: +44 (0)20 8996 7005
Email: knowledgecentre@bsigroup.com

Various BSI electronic information services are also available which give details on all its products and services.

Tel: +44 (0)20 8996 7111 Fax: +44 (0)20 8996 7048
Email: info@bsigroup.com

BSI Subscribing Members are kept up to date with standards developments and receive substantial discounts on the purchase price of standards. For details of these and other benefits contact Membership Administration.

Tel: +44 (0)20 8996 7002 Fax: +44 (0)20 8996 7001
Email: membership@bsigroup.com

Information regarding online access to British Standards via British Standards Online can be found at **www.bsigroup.com/BSOL**.

Further information about BSI is available on the BSI website at **www.bsigroup.com/standards**.

Copyright

BSI
389 Chiswick High Road
London W4 4AL
United Kingdom
www.bsigroup.com