

PAS 92:2011

Code of practice for the implementation of a biometric system

Publishing and copyright information

The BSI copyright notice displayed in this document indicates when the document was last issued.

© BSI 2011

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.

BSI retains ownership and copyright of this PAS. BSI reserves the right to withdraw or amend this PAS on receipt of authoritative advice that it is appropriate to do so. This PAS will be reviewed at intervals not exceeding two years, and any amendments arising from the review will be published as an amended PAS and publicized in *Update Standards*.

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:

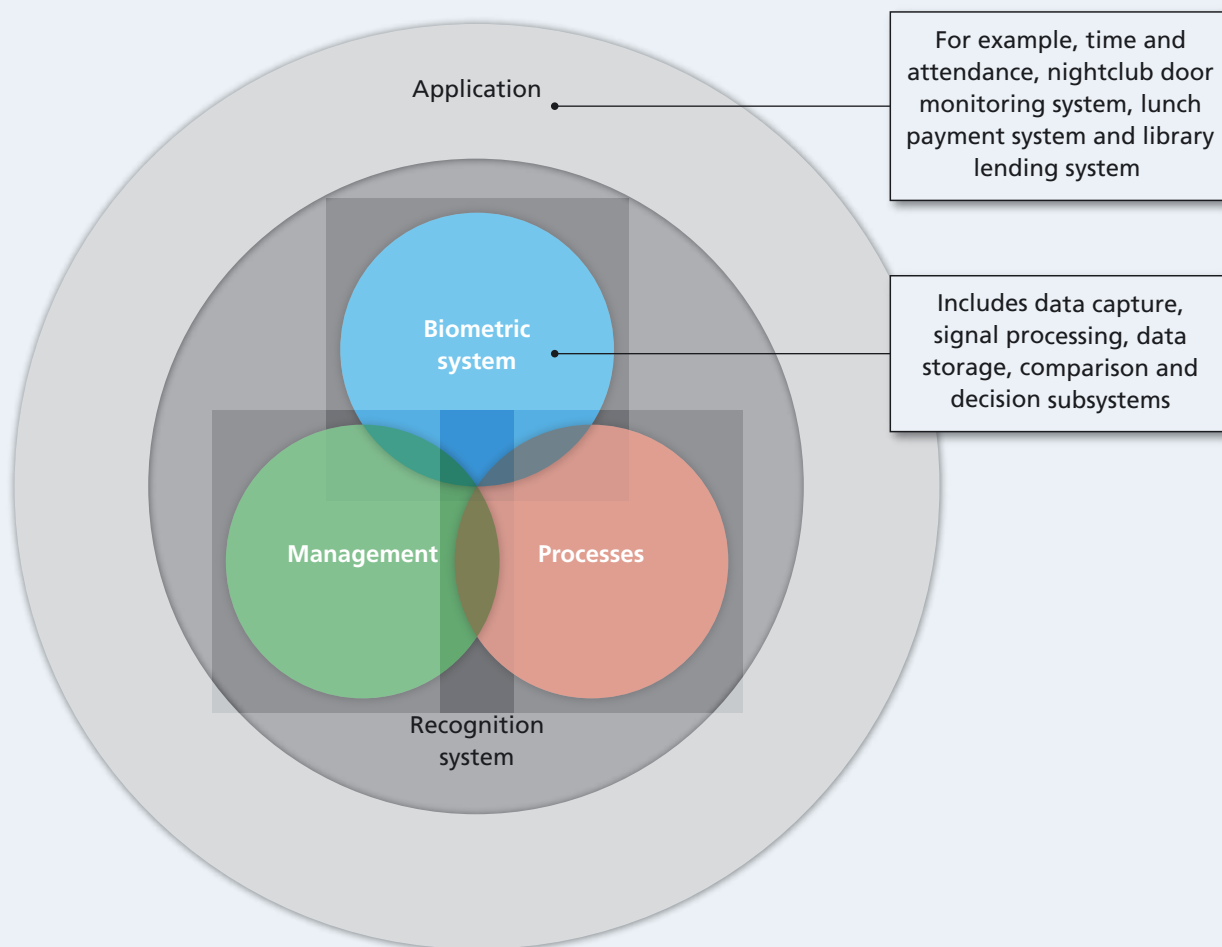
- capturing a biometric sample from an individual;
- extracting and processing the biometric data from that sample;
- storing the extracted biometric data;
- comparing the biometric data with data contained in one or more previously enrolled biometric references;
- computing how well they match; and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

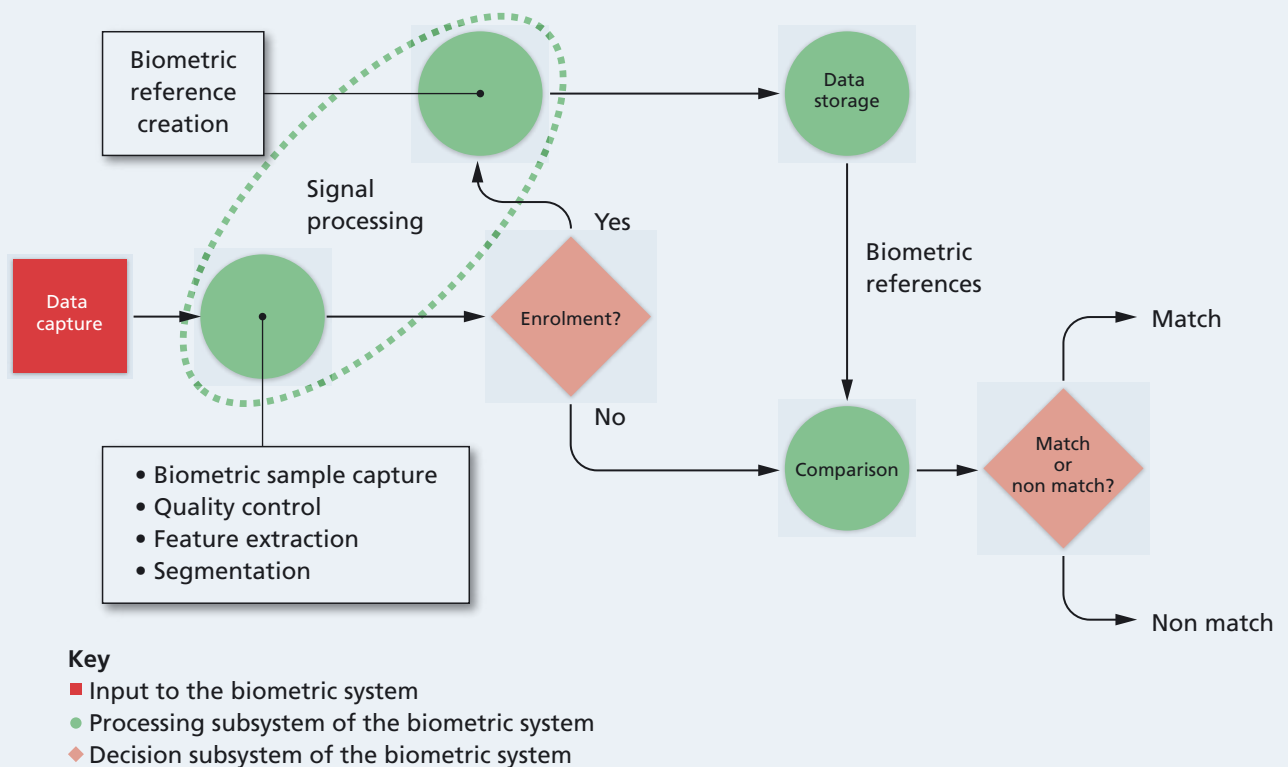
Despite the advantages of biometric recognition, biometric systems have raised public concerns. These centre on:

- 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



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 as 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.

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.

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.