TECHNICAL REPORT

ISO/IEC TR 24714-1

First edition
2008-12-15

Information technology — Biometrics — Jurisdictional and societal considerations for commercial applications —

Part 1: General guidance

Technologies de l'information — Biométrie — Considérations juridictionnelles et sociétales pour applications commerciales —

Partie 1: Guidage général

Reference number
ISO/IEC TR 24714-1:2008(E)

© ISO/IEC 2008

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2008

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

© ISO/IEC 2008 – All rights reserved

Contents

Page

Foreword iv
Introduction v
1 Scope 1
2 Terms and definitions 2
3 Symbols and abbreviated terms 3
4 Societal and cross-jurisdictional considerations 3
4.1 Introduction 3
4.2 Jurisdictional issues 3
4.3 Accessibility 10
4.4 Health and safety 13
4.5 Usability 14
4.6 Societal, cultural and ethical aspects of biometrics 17
4.7 Acceptance 18
Bibliography 22

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

In exceptional circumstances, the joint technical committee may propose the publication of a Technical Report of one of the following types:

— type 1, when the required support cannot be obtained for the publication of an International Standard, despite repeated efforts;

— type 2, when the subject is still under technical development or where for any other reason there is the future but not immediate possibility of an agreement on an International Standard;

— type 3, when the joint technical committee has collected data of a different kind from that which is normally published as an International Standard ("state of the art", for example).

Technical Reports of types 1 and 2 are subject to review within three years of publication, to decide whether they can be transformed into International Standards. Technical Reports of type 3 do not necessarily have to be reviewed until the data they provide are considered to be no longer valid or useful.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC TR 24714-1, which is a Technical Report of type 3, was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 37, *Biometrics*.

ISO/IEC TR 24714 consists of the following parts, under the general title *Information technology — Biometrics — Jurisdictional and societal considerations for commercial applications*:

— *Part 1: General guidance*

The following parts are under preparation:

— *Part 2: Specific technologies and practical applications*

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Introduction

This part of ISO/IEC TR 24714 provides support for the further development of ISO/IEC biometric International Standards in the context of cross-jurisdictional and societal applications of biometrics, including standardization of both existing and future technologies.

Specifically, this part of ISO/IEC TR 24714 offers guidance on the design of systems that use biometric technologies to capture, process and record biometric information

— with regard to societal norms and legal requirements of jurisdictional domains (within and among various levels of jurisdictions),

— pertaining to privacy/data protection of an identifiable individual,

— with respect to an individual's ability to access and use these systems and the information they contain,

— with regard to health and safety issues pertaining to an individual when systems are utilized to capture biometric data.

In this part of ISO/IEC TR 24714, biometric data are considered to be personal data.

The contents of this part of ISO/IEC TR 24714 are recommended practices and guidelines. They are not mandatory. Legal requirements of the respective countries take precedence and biometric data should be obtained in accordance with local norms of behaviour. This part of ISO/IEC TR 24714 does not reduce any rights or obligations provided by applicable laws. Compliance with any recommendations in this part of ISO/IEC TR 24714 does not of itself confer immunity from legal obligations.

Examples of the benefits to be gained by following the recommendations and guidelines in this part of ISO/IEC TR 24714 are

— enhanced acceptance of systems using biometrics by subjects,

— improved public perception and understanding of well-designed systems,

— smoother introduction and operation of these systems,

— potential long-term cost reduction (whole life costs),

— increased awareness of the range of accessibility-related issues,

— adoption of commonly approved good privacy practice.

The primary stakeholders are identified as

— users – those who use the results of the biometric data,

— developers of technical standards,

— subjects – those who provide a sample of their biometric data,

— writers of system specifications, system architects and IT designers,

— public policy makers.

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale

Information technology — Biometrics — Jurisdictional and societal considerations for commercial applications —

Part 1: General guidance

1 Scope

This part of ISO/IEC TR 24714 gives guidelines for the stages in the life cycle of a system's biometric and associated elements. This covers the following:

— the capture and design of initial requirements, including legal frameworks;

— development and deployment;

— operations, including enrolment and subsequent usage;

— interrelationships with other systems;

— related data storage and security of data;

— data updates and maintenance;

— training and awareness;

— system evaluation and audit;

— controlled system expiration.

The areas addressed are limited to the design and implementation of biometric technologies with respect to the following:

— legal and societal constraints on the use of biometric data;

— accessibility for the widest population;

— health and safety, addressing the concerns of users regarding direct potential hazards as well as the possibility of the misuse of inferred data from biometric information.

The intended audiences for this part of ISO/IEC TR 24714 are planners, implementers and system operators of biometric systems.

Specification and assessment of government policy are not within the scope of this part of ISO/IEC TR 24714.

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

2 Terms and definitions

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

2.1
accessibility
〈biometrics〉 possibility for everyone, regardless of physical capability or technological readiness, such as people with disabilities, to access and use biometric technologies and services

NOTE 1 Access can be gained directly, using assistive technologies or by the use of alternative methods. One should strive to enable direct access by as many subjects as possible (inclusive design).

NOTE 2 The ISO/IEC JTC 1 Special Working Group on Accessibility defines accessibility as “the usability of a product, service, environment or facility by people with the widest range of capabilities”.

2.2
attendant
individual who is present to guide or assist a (data) subject in enrolling or verifying their biometric data

2.3
(data) subject
individual who provides biometric data for storage or comparison in a biometric system

2.4
function creep
mission creep
expansion of a project, mission, or system’s function beyond its original goals

NOTE Function creep is the result of the intended or unintended change or extension to the functions of a system, which occur as small incremental stages, and can lead to significant changes to the function.

2.5
biometric data manager
person within the system operator’s organization accountable for compliance with the principles contained in this part of ISO/IEC TR 24714

2.6
proportionality
balance between the interests of an individual and the interests of an organisation

2.7
spoofing
〈biometric system〉 presenting a recorded image or other biometric data sample, or an artificially derived biometric characteristic, in order to impersonate an individual

2.8
usability
extent to which a product can be used by specified users (subjects) to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use

NOTE Adapted from ISO 9241-11:1998, 3.1.

2.9
personal data
information relating to an identified or identifiable individual that is recorded in any form, including electronically or on paper

--`,,```,,,,````-`-`,,`,,`,`,,`---
© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

2.10
jurisdictional domain
jurisdiction, recognized in law as a distinct legal and/or regulatory framework, which is a source of external constraints on people, their behaviour and the making of commitments between people including any aspect of a business transaction

NOTE Adapted from ISO/IEC 15944-5:2008, 3.67.

2.11
biometric data sample
data captured from a biometric sensor that can be recorded as a biometric reference for a subject or used for comparison with previously recorded biometric reference data to verify or identify a subject

3 Symbols and abbreviated terms

PET Privacy Enhancing Technology

ICT Information and Communication Technology

PDA Personal Digital Assistant

4 Societal and cross-jurisdictional considerations

4.1 Introduction

This part of ISO/IEC TR 24714 provides generic recommendations that are not specific to technologies or applications and that can affect all biometrics.

This clause begins by providing principles, guidelines and considerations for the design and implementation of biometric systems in three major areas: jurisdictional issues related to privacy and protection of personal information (4.2); accessibility (4.3); and an examination of health and safety issues when using biometric systems that may affect design and implementation considerations (4.4).

It continues with a discussion of usability addressing “real world” issues surrounding biometrics. It considers usability and highlights conditions of the physical environment that may affect the operation and usability of a biometric system (4.5).and continues with the societal, cultural and ethical aspects of biometrics (4.6); and discusses acceptance of the use of biometric characteristics (4.7).

4.2 Jurisdictional issues

4.2.1 General

The developer of a biometric system needs to take account of a number of issues that relate to specific jurisdictional requirements, which may differ between jurisdictions. Although some of these are considered in this part of ISO/IEC TR 24714, a number of others will not be examined. The list of issues which have not been examined in detail in this part of ISO/IEC TR 24714 includes

— anti-discriminatory laws,

— disclosure laws,

— redress mechanisms,

— contractual issues,

--`,,```,,,,````-`-`,,`,,`,`,,`---
© ISO/IEC 2008 All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

— provision of biometric data to other companies or subsidiaries,

— provisions for law enforcement agencies for access to biometric and associated information,

— opt-in and opt-out rights and associated requirements for fall-back processes,

— specific data retention conditions (including period of time and security standards),

— evidentiary requirements for use of biometric data in a court of law,

— specific instances where biometrics are required by organizations or governments (e.g. for secure access to military facilities and critical national infrastructure),

— applicability of legal domains in use of biometrics on the Internet,

— border control laws.

4.2.2 Privacy

With proliferation of biometric systems worldwide, the aspect of privacy gains importance. As a result it is necessary to understand what the objectives of data protection law and policy intend. It is necessary to protect not only processed data but also to protect data subjects themselves and of their personal rights. Using a biometric system means using personal data; thus existing privacy laws apply. Depending on how a system is deployed, biometric technology can compromise or protect a data subject's privacy. The possibility of protection is especially valid in view of the special properties of biometrics, which are linked uniquely to the subject for their lifetime, unlike PINs and passwords, which are only indirectly and weakly linked to a person. By using a biometric key, other types of personal data can be better protected from theft and misuse than by traditional means. Biometrics can therefore be both an object and a tool in the different aspects of this discussion. In all applications, the principle of proportionality should be applied. That means that biometric data used should be adequate, relevant and non excessive with regard to the purposes for which they are collected and further processed.

Biometrics can be considered in the context of Privacy Enhancing Technologies (PETs). PETs are a coherent system of Information and Communication Technologies (ICT) measures that protect privacy by eliminating or reducing personal data or by preventing unauthorised, unnecessary and/or undesired processing[1)] of personal data; all without losing the functionality of the data system (see Borking/Raab 2001).

The principle of PET applies to biometrics seen from two standpoints:

— as an object of the principle, the implementation and application of biometrics has to follow a comprehensive and correct privacy regime in order to be privacy enhancing;

— as a tool in the meaning of PET, biometrics itself can be a privacy enhancing method.

For instance, biometrics can improve the verification process compared with a traditional process where the subject has to give full information of his/her person along with revealing all personal information on the requested document. The use of biometrics can simply be putting a fingerprint on a sensor without revealing any additional personal information (name, address, birth date etc.) to the person who is checking the entitlement of the identified person (given that there has been a proper registration process beforehand). Moreover, the use of biometrics enables the subject to bind a device (such as a PDA) to their identity. The advantage is that the protected device cannot be used by other persons. Subjects can use pseudo-identities by varying the biometrics provided.

---

1) Processing in this context includes any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

The following are some general accepted rules of Privacy Enhancing Technologies.

— Use no personal data or as little as necessary.

— Use encryption if using personal data.

— Destroy raw data as soon as possible.

— Anonymize personal data wherever possible.

— Do not use central databases where not required.

— Give subjects control over their personal data.

— Use a means of evaluation and certification to verify that an application delivers a guarantee of an appropriate level of trust.

In relation to privacy, Article 17 of the *International Covenant on Civil and Political Rights* [36] states:

> "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation".

Privacy is one of the most significant issues confronting not only the biometrics industry, but also any organization which gathers personal information. The potential for shared access to information and multiple uses of biometric databases raises specific concerns; however, many statements on privacy fail to capture the nuances across various biometric deployments. Certain types of biometrics engender a greater perception of privacy invasion while others may have little influence on privacy concerns. Personal information is the first step to establishing personal identity and it is at this point where many crimes of identity occur. Although there are many issues associated with submitting biometric data, it should be reinforced that identification will have already been established through other identity documents such as birth certificates. Therefore, many people might consider biometric techniques to be far less invasive than being asked, sometimes face to face, a myriad of questions relating to their personal history, details of residence and information about other members of their family, such as a mother's maiden name. In this context biometric technology is simply another means for identification.

The increasing number of implementations and discussions about the use of biometrics raises questions about the technology's impact on privacy in applications generally available and widely used by the public, in the workplace and at home. Key aspects of privacy issues relate to either the data subject or the organization. From the data subject's perspective, issues relate to collection, choice, use and security of information and anonymity of the individual. From an organizational perspective, issues include the manner and purpose of collection, solicitation, storage and security of information, access to records, relevance and the limits on use and disclosure of collected data.

Other privacy issues relate to concerns that include stigmatization and reputational or financial damage . An example of stigmatization in some communities is the association of fingerprints with criminal activity; however, fingerprinting is now also becoming associated with the more positive identification of the law-abiding citizen as, a cardholder, club member and consumer. Any concerns can be exacerbated by the possibility that a person's biometric can be "spoofed".

Further privacy issues relate to function creep, or the misuse of information, and tracking or aggregation of data. In relation to function creep, using data for a secondary purpose may appear worthwhile; however, socio-cultural and legal issues may arise when individuals are not informed of this secondary purpose for which their information will be used, and have not given consent for this to take place. "Tracking" can refer to a specific form of function creep where biometric data is used in combination with additional data such as spending or travel details to track the actions of individuals. Covert use of biometrics without legal authorization will impinge on individuals' privacy.

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

In addition to the analysis of cross-jurisdictional issues relating to privacy listed in section 4.2.3, a number of other considerations may need to be taken account of, including

— issues relating to the linking of biometric data to other information;

— transition states, e.g. the ability to give consent changes:

  — migration from a minority to a majority age,

  — change in mental capacity (e.g. Alzheimer's disease),

  — death of a subject,

  — revocation procedures;

— notification to anonymously enrolled data subjects of any changes in the uses of a biometric.

The data protection officer of the system operator, or equivalent, should take part in the planning and implementation of all biometric technologies and applications and should also be included in the establishing and compliance control of the biometric privacy policy. When there is no internal data protection officer there should be a person in charge of implementing the system who is able to deal with IT security and privacy issues when they occur.

When recognized national consumer associations have published recommendations on biometrics that seem to be applicable to a specific biometric implementation, a system operator should consider them where appropriate.

4.2.3 Privacy principles for biometric systems

In certain applications biometrics allow a measure of privacy to individuals through verifying their identity rather than identifying them. They may also contribute to the enhancement of privacy in other systems by controlling access to sensitive data.

In order to protect the privacy of individuals, certain measures should be considered by organizations implementing a biometric solution.

This list builds upon the reference documents listed in Annex A, providing the user of this part of ISO/IEC TR 24714 with a minimum of commonly agreed good practice. Nevertheless, appropriate legal authorities should be consulted in order to ensure compliance with all local laws and regulations, since – in some countries – some of these principles will be mandatory and have specific obligations attached to system operators using biometric applications.

1. Transparency
   There should be a general policy of openness about the use of biometric data, which should include the purposes for which the data is to be used and the point of contact responsible for its use. Any subsequent changes should be made known to data subjects.

2. Consent
   Biometric data should be collected, used, disclosed and retained with the knowledge and consent of data subject, except where local laws have exemptions to this principle.

3. Preference for opt-in
   Where feasible and practical, opt-out or opt-in procedures should be made available to the subject. In general, opt-in is the preferred option.

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

4. Limitation of purpose
The purpose(s) of the biometric applications should be specified before implementing the biometric system, and documented and made available to affected individuals. The biometric data processing should be limited to the stated purpose[2)].

5. Limitation of collection
The collection of biometric data should be limited to the minimum required to achieve the stated purpose(s).

6. Limitation of period of retention
The biometric data should be kept only for the period of time necessary for the specified purposes. Procedures should be specified for secure removal of data that is beyond its retention period.

7. Adherence to performance criteria
The system operator should ensure the correct function and stability of the system according to its specification and that system malfunction does not cause unnecessary invasion of the subject's privacy.

8. Access rights of the data subject
The data subject should be given reasonable access to verify the correctness of the biometric data and to have incorrect data amended.

9. Protection of the data
Biometric data should be protected against unauthorized use or unlawful processing. Opportunities for such misuse should be minimized at the design and development stage of a system. Back-up and archival data should have the same level of protection as active data.

10. Secure audit
The biometric system should be designed to permit a secure audit of the use of biometric data including its deletion or removal from the biometric system. See ISO/IEC 27002:2005.

11. Data transfer between jurisdictions
As a best practice, and unless the law of the receiving jurisdiction already provides adequate protection of transfers of biometric data between jurisdictions, the system operator should take reasonable steps to ensure that the data transferred continues to be adequately protected, such as by following model contracts for the transfer of personal data such as those offered by the Article 26 (4) of directive 95/46/EC Data Protection Working Party of the European Commission[3)] , even though this may not be a legal requirement in the jurisdictions in which the organization operates.

12. Significant automated decisions
Where biometric systems are used to make significant and fully automated decisions about individuals, a mechanism to request the intervention of a person should be provided. Individuals should be notified of such automated decisions.

13. Accountability
A person within the system operator's organization should be accountable for compliance with these principles.

14. Accuracy of biometric data
Biometric information should be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

---

2) In some countries the principle of necessity is used. This requires that for use of a particular methodology or technology, especially emerging technology, it must be demonstrated that its use is required and that the purpose cannot be achieved by any other methodology and/or technology that is accepted as providing adequate protection of individuals privacy.

3) Available at <http://europa.eu.int/comm/justice_home/fsj/privacy/modelcontracts/index_en.htm>

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

15. Anonymization of data
Release of biometric data for academic, statistical or testing purposes should be considered and controlled carefully. Links to other personal information should be removed where they could lead to identification of an individual.

4.2.4 Further legal aspects

4.2.4.1 Introduction

Although this part of ISO/IEC TR 24714 is not intended to deal in detail with legal issues such as contractual or evidentiary aspects, some general statements on the legal value and potential consequences of using biometric systems will be of benefit for its audience.

In some countries a number of regulations already exist either dealing directly with use of biometrics systems or which may be applicable in this context. This section only gives a general overview of legal issues, other than privacy aspects. The detailed regulations applicable in specific countries are reported in Annex A.

4.2.4.2 Biometrics in authentication infrastructures

There is a need to facilitate electronic communication of legal transactions between parties. To achieve this many countries have introduced regulations for an electronic mechanism.

While hand-written signatures are widely accepted in the legal context, this normally relies on human signature recognition. A sample of biometric data can represent this traditional authority of the hand-written signature that complements or provides an alternative to a PIN and/or passwords.

Three factor security may involve something that a subject possesses, something they are or something they know in any combination. Two factors are sufficient for most commercial applications. In this context, biometrics characteristics in combination with digital security may be seen as the equivalence of a hand-written signature. If the use of biometrics can realise the traditional functions of the hand-written signature, a legal transaction and the binding to a person can be ensured and therefore a similar legal binding force can be achieved.

Where both the captured and reference biometrics data samples are needed to realise equivalent legal validity in transactions to that of traditional hand-written signature requires that, in all cases, both systems employed are able to deliver strong security and a reliable audit trail (see ISO/IEC 27002:2005).

The use of biometric characteristics alone in electronic transactions will be deemed by some authorities not to confer the same legal validity as a hand-written signature. In these cases biometric characteristics and digital signatures should be in a complementary relationship. Therefore, in this context, the use of biometric characteristics needs to be considered as one module in a public key infrastructure and subject to the legal requirements of that infrastructure.

4.2.4.3 Biometric methods and legal proof

The evidential value of an electronic transaction might be maximised if one or more biometric credentials are used to prevent unauthorised issue of a legal declaration.

An appropriate level of security can enhance the evidential integrity both of binding of the digital signature to the individual and in non-repudiation of the document or transaction.

Any legal challenges will best be addressed by demonstrating the reliability of the system which was used. Although the assessment of the court will differ between jurisdictions, the performance and the overall security of the biometric system will be the most significant aspect in the case.

It should be considered that recognition of a biometric data sample rarely performs perfect matching of characteristics in practical applications. It is therefore difficult to make reliable statements on the recognition quality of a specific system at a defined point in time. This contrasts with a PIN or a password where the

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

match is one hundred percent true or false but presents the risk that it might have been used by one who is not entitled to use it.

A system secured by biometric credentials is subject to similar security breaches as a system protected by PINs or passwords. Naïve faith in technology could result in a higher degree of confidence in a biometric system's security than is justified. It is therefore essential to determine the degree of security in the total system (see ISO/IEC 27002:2005).

4.2.4.4 Performance of biometric systems and liability

Biometric systems are subject not only to technical malfunction but also to reduced performance as a result of user behaviour (including operators and subjects), deliberate or accidental, or as a result of aged biometric data samples. The failure to protect and secure biometric data can incur legal liability. It is important to consider the consequences and liability issues associated with such failures in the legal context.

4.2.4.5 Standard terms of business

Liability can be dealt with in statutory provisions and also in contracts. Businesses often use pre-worded contract terms that, as a rule, add to the statutory provisions. In many countries, there are existing laws of standard terms of business, containing rules for whether such terms have become part of a contract, whether clauses are invalid, and entitle third parties (such as consumer associations) in certain circumstances to file a court claim aimed at obtaining a judgement holding a clause invalid. Generally what is often needed, is a clear and understandable wording; in other words the subject should be able to find, and familiarise himself, with certain mandatory information, without difficulty.

It is desirable to establish consumer friendly terms in order to build trust in a biometric application. Subjects are unlikely to use a biometric system for their convenience if they are disadvantaged by having the legal burden of proving whether or how they used the system in the event of a disputed match.

For instance, if the risk of malfunction of the biometric system prevents the subject's access to the protected area, standard terms of business should not shift the responsibility to the subject.

An exclusion of liability for user's system malfunctions is also usually not permitted, or at least not desirable, in terms and conditions of business. Biometric systems are vulnerable to unauthorised use and malfunctions. Besides intentional manipulations by attacks on the system and general technical problems, a certain number of potential erroneous acceptances must always be expected to occur. The subject is neither able to affect nor to control these technical aspects since these aspects are in the user's sphere alone.

4.2.4.6 Non-discrimination

Since biometrics systems use physical or behavioural information, individuals can be deterred from using them if they are unable to present the required characteristic or cannot do so in such a manner as to achieve successful verification. Examples are represented by missing fingers, inability to speak, inability to control eye movement. Considering the increasing use of biometrics this is likely to become a problem for affected subjects especially when biometrics are required to access important services.

In many countries regulations exist to prevent discrimination and to protect disabled persons. To avoid discrimination against individuals who are unable to use a particular biometric system, provisions should be made for alternative methods of identity verification.

4.2.4.7 Biometrics in the work place

In several countries specific regulations need to be taken into account when biometric technology is used for physical or logical access control in a working environment. The working place needs special consideration since the employee's ability to refuse consent is constrained by their dependence on employment. In order to protect the rights of the employees, in particular with regard to their privacy, it will often make sense to involve a workers' association, a works council, or equivalent, in place to negotiate sensible use and management of the biometric data. In Germany, for example, there are clear legal provisions which need to be considered and require the participation of the works council.

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

4.2.4.8 Aspects of criminal law

4.2.4.8.1 Altering data and unauthorised computer access

Under many criminal laws there is a prohibition of altering electronic data without authorisation and it is also not legal to access a computer of another person without appropriate entitlement. The specific cases under which legal sanctions are applicable depend on the national regulations.

4.2.4.8.2 Forgery or theft of biometric data

A spoofing attack on a system by copying or theft of biometric characteristics could be subject to criminal law in various jurisdictions. There could be a need to establish specific regulations in this regard in order to protect the wellbeing and life of subjects. Technical measures are being developed to ensure the liveness of biometric characteristics. Systems should therefore provide such a test, a verification that the biometric data sample is provided by a natural person, and include measures against “replay” or re-presentation of a sample. These features could mitigate subjects’ concerns over theft of physical biometric characteristics, and should be implemented where possible.

4.3 Accessibility

4.3.1 Introduction

A biometric system should be easily accessible to all subjects and should not disadvantage any subject. Accessibility of a biometric system is dependent on specifics of the subjects using the system and on its usability, including the physical environment (see 4.5.2). For subjects that cannot use the biometric system due to permanent or temporary conditions, alternative systems are necessary and should be provided. Any additional costs to the subject that are associated with the use of biometric applications should be clearly stated.

Accessible systems should be designed to be

— equitable in use for data subjects who have physical or psychological inabilities,

— flexible in use,

— simple and intuitive to use,

— easy-to-understand with appropriate additional prompts,

— clearly indicated by signs,

— tolerant of error,

— usable with low physical effort,

— of a size and in a space that allows easy approach and use,

— use of a range of tactile, audio and visual prompts in the user interface.

Accessibility difficulties may be long term, temporary and/or may occur without warning, for example, as the consequence of sudden onset of illness such as laryngitis or a sore throat, dental or eye surgery, or other physical injuries.

Subject groups may be internal or external to the implementing organization or may be a combination of both. It is imperative that any organization contemplating the introduction of biometrics identifies all stakeholders, considers how the subject groups might respond to the technology and identifies potential issues and solutions prior to programme implementation. Human factor issues are not confined to those who are the subjects of the technology but may also include system implementers, designers, technicians and attendants, who may all be subject to system limitations and errors.

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Reasonable efforts will need to be made to support accessibility based on analysing costs and benefits such that fewer exceptions need to be handled and less impact made on other users (operators and subjects).

Many countries have adopted inclusive policies and enforced them with legislation (e.g. the USA's Americans with Disabilities Act of 1990 [24]). Standards and Workshop Agreements on Design for All [25] are being developed at European and international level. ISO/IEC Guide 71, *Guidelines for standards developers to address the needs of older persons and persons with disabilities* [26] gives an overview on the possible impairments of subjects and helps to address their problems when standardizing and/or implementing systems. The *United Nations Standard Rules on Equal Opportunity for Persons with Disabilities* [27] provides guidelines on the enhancement of participation opportunities for people with disabilities in education, employment, social security, culture, recreation, transport and accessibility to the built environment and information. In Japan, the domestic standard (JIS X8341) with regard to the accessibility, was established in May 2004. Biometrics is described in the standard.

The system operator and/or designer should take into account the following disabilities and problems for subjects using a system. Some of these conditions can be temporary. Note also that many people have a combination of impairments, the cumulative effect of which will amplify the impact of individual impairments.

Examples of disabilities:

1. The absence of physical body parts required for the correct operation of a biometric or its specific instantiation in the system.

   Example: missing index finger(s) in an access control system using prescribed fingers

2. The absence of behavioural features required for the correct operation of a biometric or its specific instantiation in the system.

   Example: data subject with no power of speech required to use a voice-activated door entry system

3. Unusable physical body parts required for the correct operation of a biometric or its specific instantiation in the system.

   Example: person with extreme arthritis asked to use a flat plane hand geometry biometric

4. Unusable behavioural features required for the correct operation of a biometric or its specific instantiation in the system.

   Example: data subject in a country with a writing system based on non-Latin alphabet required to use a dynamic signature system designed for Latin alphabets

5. An inability to present the required biometric characteristic in a sufficiently consistent and predictable manner under the particular conditions of operation.

   Example: uncontrollable movement of the eyeball resulting in difficulty in operating an iris recognition system

   Example: person with a speech impediment (e.g. stuttering) asked to use a speaker verification scheme

6. An accelerated drift, that is a change in a characteristic over a period of time in physical or behavioural aspects resulting in increasing difficulty in meeting the matching criteria for an identification or verification.

   Example: data subject with conditions that rapidly age the facial features being verified in certain automatic face verification systems

7. An inability to access, or difficulty with physical access to, the biometric sensor or user terminal.

   Example: wheelchair data subject or person with a stature not tall enough to access a sensor or user terminal fixed at a specific height

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

8. An inability either to read, due to illiteracy, or to understand the instructions, or to recall the correct procedures, in order to operate the biometric system successfully.

Example: Forgetting which finger was enrolled in an unattended access control system, and being locked out after three attempts

9. Psychological conditions that prevent the data subject operating the biometric systems correctly.

Example: Persons with extreme compulsive-obsessive disorder required to use sensors or keypads/keyboards with physical contact

10. Conditions, such as those listed above, that result in disproportionate use of resources.

Example: Senior citizens who require a longer period of adjustment to changes in context and situation, exceeding the notional time allowed for an authentication

11. Inability to capture biometric for children or individuals that don't have "standard" size biometrics.

Example: Child using a hand geometry reader due to the position or size of the sensor.

In addition to those who are not able to use the system, there are occasions when a data subject may want to opt out of the use of the biometric and the system operator and/or designer may wish to consider granting this as an option. This option may affect the benefits of the use and the functionality of this method of authentication.

In some cases, the problems may be mitigated by changes in the design of the environment (e.g. by providing height-adjustable sensors or optimized lighting conditions). In other instances, alternative designs may need to be considered.

The approach to the design of accessible biometric systems (as well as other alternative, non-biometric approaches) will be dependent on a number of factors, including:

— whether or not the use of the system is voluntary or mandatory;

— the consequences of an adverse outcome, failure to recognise, to the subject (e.g. personal safety, financial impact, social exclusion or embarrassment, or affect on quality of life);

— the likely demographics of the target data subject group.

Designers should aim for the best overall performance for the maximum number of potential subjects, and creative and innovative design should be encouraged. The sharing of knowledge and experience of best practice should in due course lead to consistency in presentation and use of biometric systems.

Specific accessibility recommendations regarding specific technologies and applications will be given in ISO/IEC TR 24714-2 (under preparation).

4.3.2 Principles for subjects with disabilities

In order that potential data subjects with disabilities should not be disadvantaged in the application of systems using biometrics, care should be taken to design these systems to operate in accordance with the following accessibility principles.

1. Inclusive design:
   Biometric systems should be designed so that as many subjects within the target population as is reasonably possible can use the system effectively and with the minimum of discomfort. Information messages could be provided in more than one form such as visual, and audible.

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

2. Early consideration of the needs of disabled
   In the design of such new systems or services, the needs of disabled subjects should be considered from the outset.

3. Testing
   Before systems are deployed, they should be thoroughly tested by subjects who represent the widest range of abilities (that is, in respect of visual, auditory, physical, cognitive and behavioural ability).

4. Training
   For subjects with a disability, training appropriate to mitigate the disability in the use of the system should be offered.

5. Choice
   Wherever practicable, the subject should have a choice of biometric systems to use, and should not be disadvantaged if their disability prevents them from using a specific biometric.

6. Alternative method
   Where no alternative biometric technology is available and disability prevents the use of the particular biometric technology, subjects should be permitted to use an alternative method. Wherever practicable, the use of such an alternative should not result in an inferior level of service or functionality to the subject.

7. Re-enrolment
   If the subject can no longer reliably use a verification system, the subject should be provided, wherever feasible, with the opportunity to repeat the enrolment process.

8. Staff training
   Staff who operate systems that use a biometric technology should be trained in how to work with disabled subjects.

9. Consent
   A biometric system should not store details of a subject's disabilities without his or her informed consent.

10. Equality
    Rights to privacy of a disabled subject should be the same as those of a non-disabled subject.

4.4 Health and safety

4.4.1 General

The newness of biometric technologies and the lack of information and awareness by the public of these technologies and their application have generated discussion on health and safety issues. As biometric technologies become more widespread in organizations, fears that some people may already have about the use of these methods may be exacerbated by misinformation in the mass media. At an individual level, performance will be affected by these fears and perceptions, which will minimize the useful benefits of these technologies to society. To some extent, even willingness to use biometric devices will be dependent on the extent of perceived intrusiveness of the technologies in relation to health and safety issues.

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

In particular, there are two specific concerns, as follows, when considering health and safety issues in the application of biometric technologies.

— The direct medical implication of the use of biometric technologies, i.e. the potential risk for the body associated with the use of the technologies. Examples of direct medical implications are

  — physical contact with the sensing device, leading to possible infections,

  — illumination by visible or invisible light, and any potential consequent damage to a sensitive organ.

  If subjects express such health and safety concerns, these concerns usually do not reflect the reality of using these devices. Indeed many fears are not based on any scientific foundations. Nevertheless, because of these concerns, the successful implementation of biometric systems will often require that subjects be informed of any possible risk that might result from use of the device.

— Indirect medical implications reflect privacy concerns occasioned by possible health condition disclosure during a biometric process. This means data which are not needed for the actual biometric process but, under some specific circumstances or with additional processing or analysis, could give information about an extraordinary state of the subject.

  Subjects may be concerned that medical information derived from such data could affect their life insurance and employment situation, particularly if biometric information is shared or accessed between organizations.

4.4.2 Addressing the health and safety issues

To the extent that there are real threats to health and safety, the designer and system operator of the biometric system should consider the following issues.

— Biometric devices should conform to health and safety standards, where applicable and reference these standards. Subjects should be informed of any potential health and safety implications.

— In specific environments where contagions or harmful substances are present, precautions should be taken to reduce the risk of cross-contamination to acceptable levels.

4.4.3 Special cases

There may be people who experience particular psychological or physical sensitivity in the use of a particular method. While these are not easy to anticipate, system operators should be aware of the effect of such sensitivities on the performance of biometric systems. System operators should be prepared to provide accommodation where possible.

Consideration should also be given to specific environments such as hospitals, where for example medical staff cannot use fingerprint systems due to the requirement for scrupulous hand hygiene. Other examples include abattoirs, food service or manufacturing industries, pharmaceutical industries and border control and quarantine organizations where contact may be made with non-health assessed individuals. The requirement to wear protective clothing for occupational, health and safety or climatic reasons may also affect the integration of biometric technologies.

4.5 Usability

4.5.1 Introduction

Usability of a biometric system is key to optimal performance. This is equally valid for mandatory and voluntary biometric applications.

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

In 4.5.2, some aspects regarding the usability of biometric applications are presented. This list does not cover all of them. Moreover, for each of the possible biometric methods, specific usability issues will have to be considered. These will be addressed in ISO/IEC TR 24714-2 (under preparation).

The effect of these factors will vary considerably according to the specific biometric technology being used and the application in which it is deployed.

Aging of a subject will impact the performance of verification when comparing with an unchanged biometric reference. The subjects' capability to use the biometric system may also degrade with age.

4.5.2 Usability and the context of use

4.5.2.1 Introduction

The success of biometric systems is dependent on the physical environment in which they operate. Problems can be created by extremes of climate, contamination from dust or chemicals, the need for protective clothing and exposure to 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 level of verification rates is dependent upon the quality of the enrolled biometric sample which requires ideal conditions for its enrolment. Certain biometric modalities also necessitate similar conditions for enrolment and verification such as the environment for facial recognition. In this case it is important that the environments in which enrolment and everyday use take place are sufficiently similar in order to avoid a significant effect on verification rates. These biometric modalities should be carefully considered before anticipating their use in non-ideal conditions. Different environmental parameters are important for different biometric modes; and will be considered in ISO/IEC TR 24714-2 (under preparation).

The physical environment in which biometrics operate has an effect on the performance and usability of biometric systems, e.g. there should be clear instructions, documentation for subjects and reassurance on the use of data and the health and safety aspects of the technology.

4.5.2.2 Climate

Climate may present problems to sensitive biometric devices if they are subject to extreme environmental conditions such as temperatures or humidity. In outdoor locations this could include exposure to fog, rain or snow and ice or condensation on a sensor such as a camera lens. Data subjects may have to remove gloves, hats, scarves or sunglasses. Extreme temperatures may cause the biometric data sample to be more dry or moist depending on the environment. High temperatures could cause the subject to sweat and could impede the capture of the biometric data. For example, a facial verification may be adversely affected by presence of sweat on the user's face. Extremely dry environments may not allow the optimal capture for fingerprints.

4.5.2.3 Contamination

Contamination from dust or chemicals may require unusually high maintenance activity to prevent corrosion of devices and to keep devices clean. This could occur in engineering or industrial locations or in locations where food is prepared and there are high levels of oil particles from food frying. In some environments a special enclosure for the device may be required.

Protective clothing may present problems for biometric devices when they take measurements, e.g. hard hats, protective glasses, goggles and welders' masks, face masks that cover the mouth and nose, rubber or other protective gloves, and heavy boots or knee protectors that could modify a subject's posture.

4.5.2.4 External or public areas

Devices in external locations or internal public spaces may be subject to various challenges, e.g. vandalism, including attack with a heavy or sharp object or by spray-paint. High levels of ambient noise from people, machinery, public address systems or traffic may prevent voice biometrics from being collected or verified. and may also prevent users and subjects from hearing spoken instructions, which will be specially problematic for blind or partially sighted subjects who rely on these instructions.

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

In many public areas it may be necessary to provide booths or kiosks where the environment can be controlled to enable the required verification levels to be achieved.

4.5.2.5 Location

Location of biometric devices is important where active participation by the subject is required. The place where the device is located should be clearly indicated by signs, which should ideally be illuminated and have smart-sign capability to alert blind and other people with disabilities to their presence. Textured floors may also guide blind and partially sighted people to the device.

For attended applications the location of the biometric sensor should allow the actual biometric capture operation to be in full view of the attendant.

The device location should also prevent background interference during the biometric capture but should allow assistance for children by adults or for disabled people by a caregiver.

Some applications present particular challenges in locating the biometric sensor. For example, a vehicle based system where passengers in the car are required to verify their biometric data. Or if only verifying the driver, the variance in height of the vehicle would have to be taken into account for facial recognition.

Selection of the appropriate biometric for subjects in locations where people with temporary injuries congregate, e.g. a hospital accident department, needs detailed requirements captured based upon an analysis of the nature and frequency of their injuries, and in advance of design and procurement of the biometric system and especially where enrolment as well as verification, is being considered.

4.5.2.6 Throughput and data subject population

Consideration should be given to peak throughput in a location, queue management, the number of biometric devices needed and the time required, and its variability, for successful enrolment and/or positive or negative verification. The nature of the data subject population should be considered when selecting an appropriate biometric for the system.

4.5.2.7 Position

The position and orientation of biometric devices is important and consistency between the enrolment and verification systems is, in most cases, an essential requirement. The devices should be accessible to the subject community and located in a consistent position. There should be guidance on the position in which the subject should stand or sit when using the device, and variations in the subject's height and reach should be accommodated. Ideally there should be some feedback to the subject on his or her correct orientation, placement or volume in the case of a voice-based system.

4.5.2.8 Information and education

User guides should be available near public biometric devices. A helpline number or address should be displayed in a prominent position adjacent to the facility for use in the case of failure of the system or of the subject to use it successfully. Users in business or domestic environments should be trained to ensure they are familiar with the device before they approach it to perform essential tasks. The enrolment personnel will need specific training to enrol subjects in an appropriate manner.

4.5.2.9 Ease of use

The user interface of a biometric device requiring active participation by the data subject should be intuitive. The sequence of actions should be logical if the data subject is required to present his or her biometric characteristics and is also required to present a token, e.g. a smartcard, or entering an identity or account number. This may need to be researched in order to ascertain data subject expectations and using*(?)* appropriate standards. Instructions should be provided in visual and audible form, and graphical and/or visual or audible cues should prompt actions. The data subject may be required to take some action to indicate that he or she is in position and ready to present his or her biometric data. Feedback should indicate success or

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

failure and prompt a retry where appropriate. (Note. In some environments it is possible to capture biometrics passively and without the subject having to actively participate in the capture process. For example, while the subject is reading the screen a facial biometric verification is being performed. The subject should be made aware that biometric verification takes place in this environment.)

4.5.2.10 Support

Assistance should be provided especially where the operation of a biometric device is unattended and success is required for the data subject to progress. In the event of problems in presenting biometric data or with some other operation of the device, a help facility should be available to allow the subject to ask for assistance from a person either remotely or on site. Alternatively the subject should be able to invoke other procedure, e.g. on a building access system this may be a doorbell or buzzer. In a domestic context the data subject will need to have access to an override procedure in the event of injury or an activity which prevents him or her from presenting biometric data. An override procedure should also be available for use in emergencies.

4.5.2.11 Further issues

In addition to these issues levels of illumination, whether from artificial or natural light, can affect verification rates for some biometric techniques and the usability of a system. In addition vibration and motion of the system's operating environment should be considered.

4.6 Societal, cultural and ethical aspects of biometrics

This section considers societal, cultural and ethical effects on biometric solutions taken together as a whole.

Social, cultural and ethical aspects that affect biometric applications are influenced by legislative, political, emotional and economic issues. Although the diversity of these aspects within and especially across jurisdictions is extremely great, the set of privacy principles given in section 4.2.3 provides a minimum of commonly agreed good practice.

The technical limitations of any particular biometric technology should not lead to discrimination against any particular ethnic or social group.

In addition to topics already discussed in this part of ISO/IEC TR 24714, the following should be considered.

4.6.1 Commonalities and diversities

While some cultural, social and ethical aspects may be common among cultures, there are also differences which may affect biometric applications. For example most cultures currently accept photographic evidence of identity and therefore may accept biometric face recognition. In contrast individuals in some cultures may have strong objections to touching shared surfaces like fingerprint sensors or hand geometry units.

4.6.2 Multinational environments

When proposing a biometric system for a multinational user population, for example for a time and attendance application, metaphors and imagery appropriate for the respective cultural groups should be included in all information and training material.

4.6.3 Anonymity

The desire for anonymity varies among individuals in different cultural and application contexts and therefore biometric systems should be configured to offer flexibility in the degree of anonymity provided. For example some biometric applications do not necessarily need to know the personal details of a subject. They may only need to verify entitlement or prevent multiple enrolments.

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

4.6.4 Clothes, ornaments and traditions

In some cultures the individuals may be reluctant to use biometric technologies as they believe that these seriously compromise their cultural, social and ethical practices or beliefs.

For example a biometric system that relies on facial recognition could be in disharmony with a culture in which the normative behaviour is to wear a veil or head scarves. A biometric system that is negatively influenced by cultural or socially related body ornamentation (e.g., make-up, tattoos, jewellery, clothing or facial hair) may not be practical or highly acceptable.

4.6.5 Compulsory participation

Some biometric applications may require compulsory participation. The extent to which this is acceptable may depend on cultural and social demographics. For example enrolling in and using a biometric system may be a prerequisite to obtaining employment or entering a secure location.

In summary, the issues surrounding cultural, social and ethical aspects of biometrics are complex, vary both in content and across national boundaries. It is incumbent on those responsible for biometric programs to be sensitive to such distinctions. Awareness and careful consideration of the cultural, social and ethical aspects of biometrics are therefore prerequisites for all phases of biometric system implementations.

4.7 Acceptance

4.7.1 General

A crucial aspect for the success of biometric implementations is acceptance of the systems by the subjects who are to use them. As biometric uses increase, it will be important to assess the public's evolving view on the technology, its applications and its observance of privacy protection. If individuals do not accept the system, observations of projects and real world applications indicate that the overall performance will be poor. This does not depend on whether the use of the system is mandatory or voluntary. Even within a compulsory system, individuals can reject the system with non-cooperative behaviour that, over time, is likely to result in a substantial decrease in recognition rates. Therefore, it is crucial to be aware of the factors which determine acceptance, this includes positive and negative aspects. It is necessary to know how acceptance can be increased and which factors lead to less acceptance by subjects. The interaction between a user and a biometric system can only work successfully where it results in efficient and effective completion of the desired task. This interaction takes place in a particular context which includes not only a physical and organisational but also a cultural environment. This context affects the interaction and vice versa.

Concerns can be categorised as logically founded or deep-seated subjective concerns. Many technical people will be comfortable with the first group, but not realise the need to address the less tangible aspects.

Literature and project surveys describe a number of factors which can have an impact on the acceptance of a biometric system or application:

— privacy/data protection;

— convenience;

— reliability and performance;

— consumer-friendly legal conditions;

— ease-of-use;

— cost-performance-ratio;

— life-cycle;

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

— invasiveness;

— health and hygiene;

— religion, ethic and culture.

The maximum acceptance can be achieved if the biometric application is of the greatest tangible benefit for the subject. On the contrary, if the subject does not see any benefit by using the system, the willingness to use it and thus the overall acceptance of the application will decrease substantially. Moreover, the less tangible the benefit for the subject, the less willing he or she will be to accept potential risks caused by the use of the biometric system.

For biometrics to be successful in general, it is desirable that the solution reduces physical and / or in particular mental workload on subjects. Whilst biometrics have an inherent advantage over knowledge-based mechanisms, this advantage can only be realised if certain preconditions are met. Moreover it has to be considered that the use of a physical characteristic is viewed as more intimate and personal than a PIN or a password. Fear and shame can cause negative reaction to the system, and there is a need of non-discriminating use (e.g. individuals who are not able to use the system need to have a back-up and must be protected against negative gossip e.g. at the workplace). To be rejected from a biometric system may embarrass the subject, especially if this happens repeatedly and if this causes delay to other people, and thus reduce acceptance of the system or the technology in general.

In addition to the acceptance factors listed above, other success factors that have been identified include: that a biometric system

— provides a good fit to the production and security tasks that subjects have to carry out, i.e. integrated into the work process;

— performs well (high speed, low error rates) at all stages of use (installation, registration, daily use, contingency);

— is trusted to be safe, keeping the biometric data securely and not using them for other purposes.

Transparency of the overall system for the subject is another crucial success factor. Positive attitude towards biometrics might therefore be increased by higher visibility of biometric technologies in the media. The more the individual knows about the system and its details, advantages and risks, the more he or she can develop trust. Previous work on multimedia applications suggests that risks to subjects must be made explicit upfront, and users are given a choice to accept them. This goes for privacy risks, e.g. function creep, but also for health and hygiene aspects as well as issues of reliability and performance. Furthermore, trust in the user or operator of a system, of any type, is frequently a factor in the subject's trust in the system itself.

Positive attitudes towards biometrics correlate with simplicity, speed and convenience over a longer period of time. For details, see 4.5 Usability.

There are a number of trade-offs to be made, e.g. between an apparent reduction in personal privacy and a perception of increased security. Certain groups will position this trade-off at different points, and the prospective implementer and operator of a biometric system should consider the various groups within the user community.

Examples of the way in which such groups can be approached are:

— age;

— gender;

— education;

— occupation;

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

— expertise;

— culture;

— ethnicity;

— 'caring' responsibilities, e.g. parents of school age children, and people responsible for the elderly and vulnerable;

— socio-economic grouping and origin;

— attitudes to authority and previous involvement with the police.

Across the different cultures all over the world there will be significant differences in the attitude towards biometrics and different levels of information. Cultural differences might even be stronger than gender or age differences. There might be differences in the privacy assessment as well as in the rating of performance and security.

4.7.2 Privacy and acceptance

According to surveys and projects performed, privacy safeguards (or rules) seem to be critical acceptance factors for individuals who are to use biometrics. The majority of individuals who were interviewed were in favour of biometrics e.g. in order to combat identity theft, but at the same time are concerned about possible misuse of their personal information. On the other hand, there are trade-offs that people are willing to make between privacy and convenience. The success of point-of-sale, pay-by-touch systems shows that, for many people in many contexts, convenience is more important than privacy. This does not mean that privacy concerns can be ignored in such systems, and implementers should strive to provide both privacy and convenience.

Experiences indicated the greatest possible transparency is able to reduce privacy fears. This should include information in advance of the use and the reason for the use as well as information about how the biometric data are used, shared, and in which manner they are processed. People's concerns also seem to include the possible combination with other personal identifiers and the risk of tracking people's movement. Another trust factor is the ability of the individual to check that biometric data is correct.

A comprehensive security concept should require that biometric data that are used are considered as personal data and mechanisms to secure those data are provided.

4.7.3 Reliability, performance and acceptance

Where there is a lack of confidence in the accuracy and reliability of biometric technology (e.g. high throughput times, high rates of false rejection and poor user interfaces), this may result in reduced acceptance. For some social groups and cultures, fear is a normal psychological response to the unknown. High false rejection rates can lead to decreased acceptance, although this seem to depend on the applications purpose. Whereas in high security areas individuals are likely to accept more attempts to get identified, in more convenience driven applications they are probably not ready to accept more than three attempts. This also depends on the information subjects are given in advance of the implementation and use.

4.7.4 Recommended actions for acceptance testing

It is suggested that operators should consider the following factors as a minimum:

NOTE This is not a comprehensive checklist.

1. Piloting of the biometric application should be undertaken and the acceptance factors determined for all groups which will be potential subjects of the biometric system.

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

2. Check the user population for the specific application in order to address the concrete concerns of the respective subjects.

3. Planners should remember that although systems may be designed initially for early adopters and/or specific target groups, subsequent extension to other groups of subjects may require additional testing and redesign.

4. Specific aspects related to biometrics include the need for re-enrolment as people age.

5. One way to improve user acceptance would be to adjust the threshold in a biometric system in order to reduce the rate of false rejections. However, this carries a corresponding penalty of a reduction in security. The relation between false acceptance and false rejections should be explained to the subjects.

6. Provide information and usage guidelines understandable for non-technical persons and, dependent on the user population, in different languages.

7. If acceptance testing is undertaken, the subject group should be allowed to familiarise themselves with the biometric system in the context of the application.

8. Both education and marketing of the intended use of the biometric is crucial to address both the logically sound concerns and subjective cultural uncertainties.

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Bibliography

Privacy and data protection related documents

[1] National Biometric Security Project (NBSP): United States Federal Laws Regarding Privacy and Personal Data and Applications to Biometrics, June 2005; and

[2] OECD Guidelines of 1980 as a benchmark for onward development of personal data protection laws.

[3] Article 29 (EU Directive 95/45/EC) Data Protection Working Party: Working Document on Biometrics. WP80. August 2003.

[4] Article 29 (EU Directive 95/45/EC) Data Protection Working Party: Option No. 7/2004 on the inclusion of biometric elements in resident permits and visas taking account of the establishment of the European information system on visas VIS. WP96. August 2004

[5] Article 29 (EU Directive 95/45/EC) Data Protection Working Party: Opinion on implementing the council regulation (EC) No. 2252/2004 of 13. December 2004 on standards for security features and biometrics in passports and travel documents issued by member states. WP112. September 2005.

[6] Borking/Raab 2001

[7] The US Privacy Act 1974 and its implementation

[8] Australian Privacy Act 1988, including the Information Privacy Principles (IPP) for Government and the National Privacy Principles (NPP) for industry, and the (proposed) Biometrics Privacy Code

[9] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

[10] The German Federal Data Protection Act as of 1. January 2003

[11] International Security Trust & Privacy Alliance (ISTPA), *Privacy Framework*

[12] Canadian "Privacy Assessment Checklist" in the *Multi-Application Smart Cards: How to do a Privacy Assessment*, August 2000 (under revision in December 2003) (in N509)

[13] Biometrics Institute, *Privacy Code* (referred to in N509)

[14] International Data Privacy Laws and Application to the Use of Biometrics in the United States, January 2005

[15] INFORMATION AND PRIVACY COMMISSIONER/ONTARIO. *Privacy and Biometrics*, Canada, September 1999

[16] Anne Cavoukian, PhD, "Privacy and Biometrics: An Oxymoron or Time to Take a 2nd Look?" Submission to "Computers, Freedom and Privacy 1998", Austin, Texas: Minimum privacy requirements

[17] Advisory Committee on Automated Personal Data Systems, "Records, Computers, and the Rights of Citizens," DHEW Publication No. (OS) 7394, Washington, DC: U.S. Department of Health, Education and Welfare, 1973

[18] PRABHAKAR, S., PANKANTI, S. and JAIN, A.K. (2003). Biometric recognition: Security and privacy concerns. IEEE Security and Privacy, 1(2), pp. 33-42

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

[19] E.M. NEWTON, L. SWEENEY, B. MALIN. “Preserving Privacy by De-identifying Facial Images.” in *IEEE Transactions on Knowledge and Data Engineering*, February 2005, 17(2).

[20] M.G. MORGAN and E.M. NEWTON. "Protecting Public Anonymity" in *Issues in Science and Technology*, Fall 2004

[21] J.D. WOODWARD, K.W. WEBB, E.M. NEWTON, M. BRADLEY, D. RUBENSON, et al. *Army Biometric Applications: Identifying and Addressing Sociocultural Concerns*. MR-1237-A. RAND. Santa Monica, CA, 2000

[22] ISO/IEC 27002:2005, *Information technology — Security techniques — Code of practice for information security management*

Accessibility related documents

[23] In Japan, domestic standard (JIS X8341) with regard to accessibility was established in May 2004. The standard contains a description concerning biometrics

[24] UNITED STATES OF AMERICA. Americans with Disabilities Act of 1990. Public Law 101-336 of the 101st Congress, enacted July 26, 1990

[25] Workshop Agreements on Design for All

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

[27] UNITED NATIONS. *United Nations Standard Rules on Equal Opportunity for Persons with Disabilities*. 1993

[28] CWA 14661: Guidelines to Standardisers of ICT products and services in the CEN ICT domain. 2003

[29] CEN Workshop on Design for All: Final Report 05/2000

[30] UK Passport Service (2005). Biometrics enrolment trial report

Other documents relating to biometrics

[31] Biovision Final Report, Biovision Best Practices

[32] Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB) report 76, 12168/02/EN

[33] TAB No 93 *Biometrics and identity documents,* “Performance, political context, legal considerations, 2. Status report”, by Thomas Petermann, Constanze Scherz, Arnold Sauter. (Only a summary available in English)

[34] J.D. WOODWARD, Jr. “Biometric Scanning, Law & Policy: Identifying the Concerns - Drafting the Biometric Blueprint, *University of Pittsburgh Law Review*, Vol. 59, Issue 1, Autumn 1997, S. 97 ff

[35] Samir Nanavati, Michael Thieme and Raj Nanavati, *Biometrics: Identity Verification in a Networked World*, John Wiley and Sons, 2002

[36] OFFICE OF THE HIGH COMMISSIONER FOR HUMAN RIGHTS. *International Covenant on Civil and Political Rights, Adopted and opened for signature, ratification and accession by General Assembly resolution 2200A (XXI) of 16 December 1966,* entry into force *23 March 1976, in accordance with Article 49*. Geneva: OHCHR

[37] TeleTrusT e.V., BioTrusT-Report, 1999-2002

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

[38] Federation of German Consumer Organisation (vzbv): Biometrics and consumer protection, 25. Jan. 2001

[39] BENTE, G. and ESCHENBURG, F. (2005). Usability and acceptance issues in biometric security technology: The BioSec approach. Presentation to the Second BioSec Workshop, Brussels, Jan 19-20

[40] TNS/TRUSTe (2005). Consumer attitudes about biometrics in ID documents

[41] ASHBOURN, J. (2000). Biometrics: Advanced identity verification. London: Springer Verlag

[42] Citizenship & Immigration Canada (2003). Tracking public perceptions of biometrics

[43] COVENTRY, L. (2004). Fingerprint authentication: The user experience. Paper presented at the DIMACS Workshop on Usable Privacy and Security Software, July 7 - 8, Rutgers University, Piscataway, NJ

[44] COVENTRY, L. (2005). Usable biometrics. In L.F. Cranor & S. Garfinkel (Eds.), Security and usability: Designing secure systems that people can use. O'Reilly Media, Inc.

[45] Opinion Research Corporation International (2002). Public attitudes toward the uses of biometric identification technologies by government and the private sector: Summary of survey findings. Available

[46] PRAKASH, D. (2005). Consumers pay with their finger. Paper presented at the Biometric Consortium Conference, Sept. 19-21, Arlington, VA

[47] SASSE, M.A. (2004) Usability and user acceptance of biometrics. Paper prepared for the CESG/BWG Government Biometrics Workshop, London

[48] TNS/TRUSTe (2005). Consumer attitudes about biometrics in ID documents

Other documents

[49] ISO/IEC 15944-5, *Information technology — Business Operational View — Part 5: Identification and referencing of requirements of jurisdictional domains as sources of external constraints*

[50] ISO/IEC 9241-11:1998, *Ergonomic requirements for office work with visual display terminals (VDTs) — Part 11: Guidance on usability*

© ISO/IEC 2008 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

ICS 35.020

Price based on 24 pages

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2008 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale