BS ISO/IEC 24745:2011

BSI Standards Publication

Information technology — Security techniques — Biometric information protection

NO COPYING WITHOUT BSI PERMISSION EXCEPT AS PERMITTED BY COPYRIGHT LAW

raising standards worldwide™

AVA Documents BSI Document Sharing Hub

Full document details: BS ISO/IEC 24745:2011

National foreword

This British Standard is the UK implementation of ISO/IEC 24745:2011.

The UK participation in its preparation was entrusted to Technical Committee IST/33, IT - Security techniques.

A list of organizations represented on this committee can be obtained on request to its secretary.

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

© BSI 2011

ISBN 978 0 580 55573 2

ICS 35.040

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 July 2011.

Amendments issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 24745:2011

INTERNATIONAL STANDARD

ISO/IEC 24745

First edition
2011-06-15

Information technology — Security techniques — Biometric information protection

Technologies de l'information — Techniques de sécurité — Protection des informations biométriques

Reference number
ISO/IEC 24745:2011(E)

Documents
Document Sharing Hub

© ISO/IEC 2011

Full document details: BS ISO/IEC 24745:2011

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2011

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

© ISO/IEC 2011 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 24745:2011

Contents

Page

Foreword v

Introduction vi

1 Scope 1

2 Terms and definitions 1

3 Abbreviated terms 5

4 Biometric systems 6
4.1 Introduction to biometric systems 6
4.2 Biometric system operations 8
4.3 Biometric references and identity references 10
4.4 Biometric systems and identity management systems 10
4.5 Personally identifiable information and universal unique identifiers 11
4.6 Societal considerations 11

5 Security aspects of a biometric system 12
5.1 Security requirements for biometric systems to protect biometric information 12
5.2 Security threats and countermeasures in biometric systems 13
5.3 Security of data records containing biometric information 16

6 Biometric information privacy management 20
6.1 Biometric information privacy threats 20
6.2 Biometric information privacy requirements and guidelines 20
6.3 Regulatory and policy requirements 21
6.4 Biometric information lifecycle privacy management 21
6.5 Responsibilities of a biometric system owner 23

7 Biometric system application models and security 24
7.1 Biometric system application models 24
7.2 Security in each biometric application model 25

Annex A (informative) **Secure binding and use of separated DB_{IR} and DB_{BR}** 37
A.1 General 37
A.2 Secure Binding between Separated DB_{IR} and DB_{BR} 37
A.3 BR claim for verification 38
A.4 IR claim for identification 39

Annex B (informative) **Cryptographic algorithms for security of biometric systems** 40
B.1 Cryptographic algorithms providing confidentiality 40
B.2 Cryptographic algorithms providing integrity 40
B.3 Cryptographic algorithms providing confidentiality and integrity 40

Annex C (informative) **Framework for renewable biometric references** 41
C.1 Renewable biometric references 41
C.2 Creation 41
C.3 Comparison 42
C.4 Expiration 42
C.5 Revocation 42
C.6 Architecture overview 43

Annex D (informative) **Technology examples for renewable biometric references** 44
D.1 Overview 44

Documents
Document Sharing Hub

© ISO/IEC 2011 – All rights reserved

Full document details: BS ISO/IEC 24745:2011

Annex E (informative) **Biometric watermarking** **46**
E.1 Biometric watermarking **46**
E.2 Insertion and extraction of a biometric watermark **46**
E.3 Application examples **47**

Bibliography **48**

© ISO/IEC 2011 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 24745:2011

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.

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 24745 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

© ISO/IEC 2011 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24745:2011

Introduction

As the Internet becomes a more pervasive part of daily life, various services are being provided via the Internet, such as Internet banking, remote healthcare, etc. In order to provide these services in a secure manner, the need for authentication mechanisms between subjects and the service being provided becomes even more critical. Some of the authentication mechanisms already developed include token based schemes, personal identification and transaction numbers (PIN/TAN), digital signature schemes based on public key cryptosystems, and authentication schemes using biometric techniques.

Biometrics – the automated recognition of individuals based on their behavioural and physiological characteristics – has come of age, and includes recognition technologies based on fingerprint image, voice patterns, iris image, facial image, and the like. The cost of biometric techniques has been decreasing while their reliability has been increasing, and both are now acceptable and viable for use as an authentication mechanism.

Biometric authentication introduces a potential discrepancy between privacy and authentication assurance. On the one hand, biometric characteristics are ideally an unchanging property associated with and distinct to an individual. This binding of the credential to the person provides strong assurance of authentication. On the other hand, this strong binding also underlies the privacy concerns surrounding the use of biometrics, such as unlawful processing of biometric data, and poses challenges to the security of biometric systems to prevent the compromise of biometric references. The usual solution to the compromise of an authentication credential – to change the password or issue a new token – is not generally available for biometric authentication because biometric characteristics, being either intrinsic physiological properties or behavioural traits of individuals, are difficult or impossible to change. At most another finger or eye could be enrolled, but the choices are usually limited. Therefore, appropriate countermeasures to safeguard the security of a biometric system and the privacy of data subjects are essential.

Biometric systems usually bind a biometric reference with other personally identifiable information (PII) for authenticating individuals. In this case, the binding is needed to assure the security of the data record containing biometric information. The increasing linkage of biometric references with other PII and the sharing of biometric information across legal jurisdictions make it extremely difficult for organizations to assure the protection of biometric information and to achieve compliance with various privacy regulations.

© ISO/IEC 2011 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24745:2011

INTERNATIONAL STANDARD ISO/IEC 24745:2011(E)

Information technology — Security techniques — Biometric information protection

1 Scope

This International Standard provides guidance for the protection of biometric information under various requirements for confidentiality, integrity and renewability/revocability during storage and transfer. Additionally, this International Standard provides requirements and guidelines for the secure and privacy-compliant management and processing of biometric information.

This International Standard specifies the following:

— analysis of the threats to and countermeasures inherent in a biometric and biometric system application models;

— security requirements for securely binding between a biometric reference and an identity reference;

— biometric system application models with different scenarios for the storage and comparison of biometric references; and

— guidance on the protection of an individual's privacy during the processing of biometric information.

This International Standard does not include general management issues related to physical security, environmental security and key management for cryptographic techniques.

2 Terms and definitions

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

2.1
authentication
process of establishing an understood level of confidence that a specific entity or claimed identity is genuine

NOTE 1 Authentication includes the process of ascertaining an understood level of confidence of the truth of a claimed identity before the entity can be registered and recognized in a domain.

NOTE 2 Although this definition is generic, its use within this International Standard is limited to the biometric authentication of human subjects.

[ISO 19092:2008]

2.2
auxiliary data
AD
subject-dependent data that is part of a renewable biometric reference and may be required to reconstruct pseudonymous identifiers during verification, or for verification in general

NOTE 1 If auxiliary data is part of a renewable biometric reference, it is not necessarily stored in the same place as the corresponding pseudonymous identifiers.

© ISO/IEC 2011 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24745:2011

NOTE 2 Auxiliary data may contain data elements for diversification (i.e. diversification data).

NOTE 3 Auxiliary data is not the element for comparison during biometric reference verification.

NOTE 4 Auxiliary data are generated by the biometric system during enrolment.

EXAMPLE Secret number encrypted by a key derived from a biometric sample using a helper data approach, fuzzy commitment scheme, or fuzzy vault. See Annex D, Table D.1 for concrete examples of PI and AD.

2.3
biometric characteristic
physiological or behavioural characteristic of an individual that can be detected and from which distinguishing, repeatable biometric features can be extracted for the purpose of automated recognition of individuals

[ISO/IEC JTC 1/SC 37 SD2 (v.11)]

2.4
biometric data
biometric sample, biometric feature, biometric model, biometric property, other description data for the original biometric characteristics, or aggregation of above data

[ISO/IEC JTC 1/SC 37 SD2 (v.11)]

2.5
biometric data subject
subject
individual whose biometric reference is within the biometric system

2.6
biometric feature
numbers or labels extracted from biometric samples and used for comparison

[ISO/IEC JTC 1/SC 37 SD2 (v.11)]

2.7
biometric information privacy
right to control the collection, transfer, use, storage, archiving, disposal and renewal of one's own biometric information throughout its lifecycle

2.8
biometric model
stored function (dependent on the biometric data subject) generated from a biometric feature or features

NOTE Comparison applies the stored function to the biometric features of a probe biometric sample to give a comparison score.

EXAMPLE Examples of stored functions include Hidden Markov Models, Gaussian Mixture Models or Artificial Neural Networks.

[ISO/IEC JTC 1/SC 37 SD2 (v.11)]

2.9
biometric property
descriptive attributes of the biometric data subject estimated or derived from the biometric sample by automated means

EXAMPLE Fingerprints can be classified by the biometric properties of ridge-flow (i.e. arch, whorl, and loop types); face images can be used for estimating age or gender.

[ISO/IEC JTC 1/SC 37 SD2 (v.11)]

© ISO/IEC 2011 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24745:2011

2.10
biometric reference
BR
one or more stored biometric samples, biometric templates or biometric models attributed to a biometric data subject and used for comparison

NOTE A biometric reference that can be renewed is referred to as a renewable biometric reference.

EXAMPLE Face image on a passport; fingerprint minutiae template on a National ID card; Gaussian Mixture Model, for speaker recognition, in a database.

[ISO/IEC JTC 1/SC 37 SD2 (v.11)]

2.11
biometric sample
analog or digital representation of biometric characteristics obtained from a biometric capture device or biometric capture subsystem prior to biometric feature extraction

[ISO/IEC JTC 1/SC 37 SD2 (v.11)]

2.12
biometric system
system for the purpose of the automated recognition of individuals based on their behavioural and physiological characteristics

2.13
biometric template
set of stored biometric features comparable directly to probe biometric features

2.14
claim
assertion of identity

2.15
claimant
individual making a claim of identity

NOTE Claims can be verified in a number of ways, some of which may be based on biometrics.

2.16
common identifier
identifier for correlating identity references and biometric references in physically or logically separated databases

2.17
diversification
deliberate creation of multiple, independent, transformed biometric references from one or more biometric samples obtained from one data subject for the purposes of security and privacy enhancement

2.18
identification
⟨biometrics⟩ process of performing a biometric search against an enrolment database to find and return the identity reference attributable to a single individual

2.19
identifier
one or more attributes that uniquely characterize an entity in a specific domain

EXAMPLES The name of a club with a club-membership number, a health insurance card number together with the name of the insurance company, an IP address, and a universal unique identifier.

Documents
Document Sharing Hub

© ISO/IEC 2011 – All rights reserved

Full document details: BS ISO/IEC 24745:2011

2.20
identity
set of properties or characteristics of an entity that can be used to describe its state, appearance or other qualities

2.21
identity management system
IdMS
system controlling entity identity information throughout the information lifecycle in one domain

2.22
identity reference
IR
non-biometric attribute that is an identifier with a value that remains the same for the duration of the existence of the entity in a domain

2.23
irreversibility
property of a transform that creates a biometric reference from a biometric sample(s) or features such that knowledge of the transformed biometric reference cannot be used to determine any information about the generating biometric sample(s) or features

2.24
personally identifiable information
PII
any information

— that identifies or can be used to identify, contact, or locate the person to whom such information pertains,

— from which identification or contact information of an individual person can be derived, or

— that is or might be directly or indirectly linked to a natural person

[ISO/IEC 29100:—[1)]]

2.25
pseudonymous identifier
PI
part of a renewable biometric reference that represents an individual or data subject within a certain domain by means of a protected identity that can be verified by means of a captured biometric sample and the auxiliary data (if any)

NOTE 1 A pseudonymous identifier does not contain any information that allows retrieval of the original biometric sample, the original biometric features, or the true identity of its owner.

NOTE 2 The pseudonymous identifier has no meaning outside the service domain.

NOTE 3 Encrypted biometric data with a cipher that allows retrieval of the plain-text data is not a pseudonymous identifier.

NOTE 4 A pseudonymous identifier is the element for comparison during biometric reference verification.

NOTE 5 See Annex D, Table D.1 for examples of PI and AD.

1) To be published.

© ISO/IEC 2011 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24745:2011

2.26
pseudonymous identifier encoder
PIE
system, process or algorithm that generates a renewable biometric reference consisting of a pseudonymous identifier (PI) and possibly auxiliary data (AD) based on a biometric sample or biometric template

2.27
renewability
property of a transform or process to create multiple, independent transformed biometric references derived from one or more biometric samples obtained from the same data subject and which can be used to recognize the individual while not revealing information about the original reference

2.28
renewable biometric reference
revocable or renewable identifier that represents an individual or data subject within a certain domain by means of a protected binary identity (re)constructed from the captured biometric sample

NOTE A renewable biometric reference consists of a pseudonymous identifier and additional optional data elements required for biometric verification or identification such as auxiliary data.

2.29
revocability
ability to prevent future successful verification of a specific biometric reference and the corresponding identity reference

NOTE Rejection of an entity may occur on the grounds of its appearance on a revocation list.

2.30
secure channel
communication channel providing the confidentiality and authenticity of exchanged messages

2.31
token
physical device storing biometric reference and in some cases performing on-board biometric comparison

EXAMPLES Smart card, USB memory stick or RFID chip in e-passport.

2.32
unlinkability
property of two or more biometric references that they cannot be linked to each other or to the subject(s) from which they were derived

2.33
verification
⟨biometrics⟩ process of confirming a claim that an individual who is the subject of a biometric capture process is the source of a claimed identity reference

3 Abbreviated terms

AD Auxiliary Data

AFIS Automated Fingerprint Identification Systems

BR Biometric Reference

BIR Biometric Information Record

CI Common Identifier

© ISO/IEC 2011 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24745:2011

OCC	On-Card Comparison
DB_{BR}	Database containing Biometric Reference
DB_{IR}	Database containing Identity Reference
IdMS	Identity Management System
IR	Identity Reference
MAC	Message Authentication Code
PDA	Personal Digital Assistant
PET	Privacy Enhancing Technology
PI	Pseudonymous Identifier
PIC	Pseudonymous Identifier Comparator
PIE	Pseudonymous Identifier Encoder
PII	Personally Identifiable Information
PIR	Pseudonymous Identifier Recoder
RBR	Renewable Biometric Reference
RFID	Radio Frequency Identification
TTP	Trusted Third Party
USB	Universal Serial Bus
UUID	Universal Unique Identifier
$\xrightarrow{x}$	An arrow represents either a simple information flow of data *x* or initiation of an interactive protocol whose exchanged data may depend on the whole or a part of *x*.

NOTE 1*x* may be encrypted when a secure messaging system such as ISO/IEC 7816-4 is used.
NOTE 2The interactive protocol may not transfer any information on *x* when, for example, a zero-knowledge technique is used.

4 Biometric systems

4.1 Introduction to biometric systems

Biometric systems perform the automated recognition of individuals based on one or more physiological (physical properties of the body such as fingerprints) and/or behavioural (things an individual does, such as walking) characteristics.

Physiological characteristics include but are not limited to:

— fingerprint,
— face,
— iris,
— hand geometry,
— hand/finger vein,
— retina,

© ISO/IEC 2011 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24745:2011

— DNA, and

— palm print,

and behavioural characteristics include but are not limited to:

— signature,

— gait, and

— voice.

The following are desirable properties of biometric characteristics that lead to good subject discrimination and reliable recognition performance [4]:

— universality: Every individual should have the characteristic;

— uniqueness: Every individual should have a distinguishable characteristic;

— permanence: The characteristics should not show variance with time, e.g. variance over time;

— collectability: The characteristics should be easily collected from the subjects; and

— repeatability: The characteristics should be sufficiently distinct and repeatable to achieve successful recognition of the subject.

From an application point of view, the following additional properties should also be taken into account:

— performance, which mainly refers to the success rate in recognizing individuals;

— acceptability, which represents the level of willingness by the subject to use the biometric system; and

— spoof resistance, which indicates how difficult it is to use a replica of the biometric characteristic to circumvent the biometric system.

For verifying and/or identifying an individual a biometric system processes one or more probe samples for comparison against stored biometric reference(s). The biometric reference could be a biometric sample (e.g., an image representing the biometric characteristic) or a set of biometric features (i.e., a template that is derived from the image) or it could be a biometric model composed from the features.

Specifically, physiological biometric characteristics are very difficult to alter, so their compromise can have permanent consequences for the individual in applications in which immutability of the characteristic is assumed.

© ISO/IEC 2011 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24745:2011

4.2 Biometric system operations

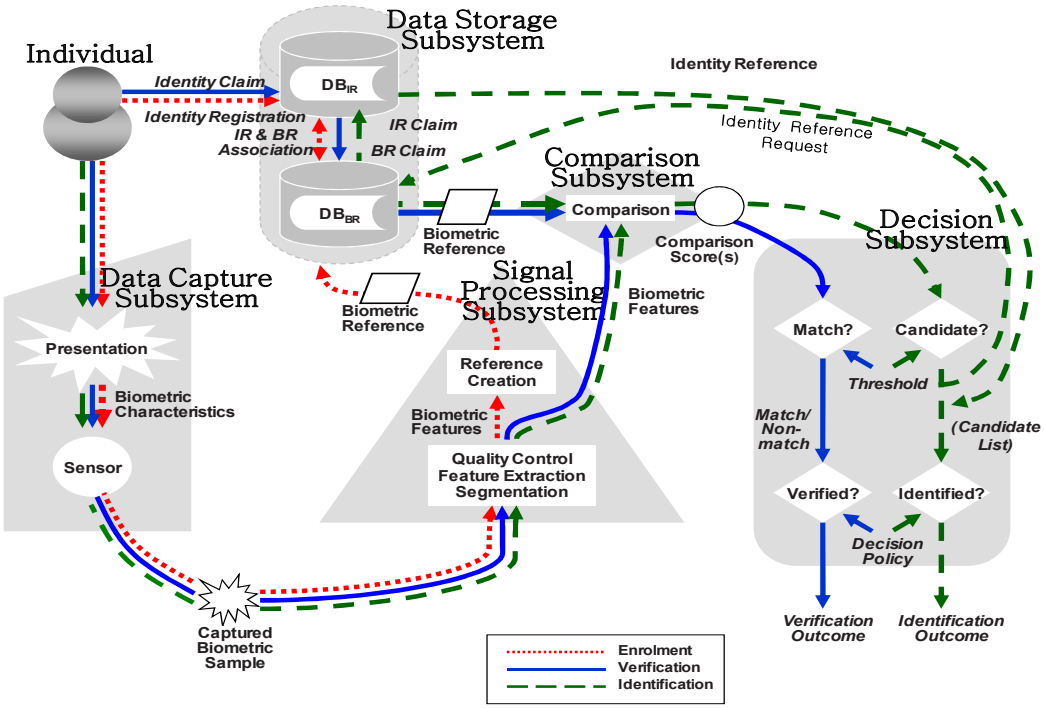

Figure 1 — Conceptual structure of a biometric system

The overall operation of a biometric system is depicted in Figure 1, which is an expanded version of the original one given in ISO/IEC SC37 SD11 [18], to highlight the processing of the identity reference.

The biometric system usually consists of five subsystems.

— A biometric data capture subsystem, which contains biometric capture devices or sensors for collecting signals from a biometric characteristic and converting them into a biometric sample such as a fingerprint image, facial image or voice recording.

— A signal processing subsystem, which extracts biometric features from a biometric sample with the intent of outputting numbers or labels which can be compared with those extracted from other biometric samples. Here, the biometric feature extracted in the enrolment process is stored in the data storage subsystem as a biometric reference for the identification and verification process.

— A data storage subsystem, which serves primarily as an enrolment database where the linking of the enrolled biometric references to the identity reference occurs. The data may contain biometric data and also non-biometric data such as the identity reference related to the subject. In practice, DB_{IR} and DB_{BR} are often logically or physically separated for reasons of security and privacy concerns. A more detailed description of binding DB_{IR} with DB_{BR} is given in Annex A.

— A comparison subsystem, which determines the similarity between captured biometric samples (or derived features) and stored biometric references. In the case of the one-to-one comparison used in the verification process, a captured biometric sample is compared with a stored biometric reference from a biometric data subject to produce a comparison score. However, in the one-to-many comparison used in the identification process, an extracted feature of a biometric data subject is compared against a set of biometric references of more than one biometric data subject to return a set of comparison scores.

© ISO/IEC 2011 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24745:2011

— A decision subsystem, which determines whether the captured biometric sample and the biometric reference have the same source (biometric subject), based on a comparison score(s) and a decision policy (or policies) including a threshold. In the case of the verification process, the biometric data subject may be accepted or rejected according to the comparison score. In the case of identification, a list of candidate identities that meet the decision policy is presented.

In essence, a biometric system involves three main functional processes:

— Enrolment process: creating and storing an enrolment data record for an individual who is the subject of a biometric capture process in accordance with the enrolment policy. The subject usually presents his/her biometric characteristics to a sensor along with his/her identity reference. The captured biometric sample is processed to extract the features which are enrolled as a reference in the enrolment database with the identity reference.

— Identification process: searching the enrolment database against the captured and extracted biometric features to return a candidate list. The candidate list consists of individuals whose references match with the feature in the comparison subsystems and have a similarity score value higher than a predefined threshold value.

— Verification process: testing a claim that an individual who is the subject of a biometric capture process is the source of a specified biometric reference. The subject presents his/her identity reference for a claim of identity and also their biometric characteristic(s) to the capturing device, which acquires biometric sample(s) to be used for comparison with the biometric reference linked to the identity reference for the claimed identity.

The verification process has a possibility of impacting on the subject's information privacy since this process requires both biometric reference and identity reference. The identification process requires exhaustive search of the enrolment database. So, this also has a possibility of impacting on the subject's physical privacy. Verification is generally considered to be less privacy intrusive than identification.

The five abovementioned subsystems represent the technical and functional blocks that capture, process, store, compare, and decide on the processing of biometric data. In addition, other functional subsystems can be included [7].

— A reference-adaptation subsystem, which modifies a reference using a new biometric feature, extracted from a successful verification or identification process. Adaptation is generally employed by biometric systems to reflect external factors and to minimize their effects on the recognition rate. It may also be used for attenuating the potential effects of reference aging. Unsupervised adaptation can be performed automatically based upon a pre-determined policy. Supervised adaptation is usually invoked by the application and is based on application-specific criteria. For example, it may be called upon when the biometric comparison score is not high but other factors clearly support the asserted identity. Since a lower comparison score may cause the system to reject a genuine user, adoption of a reference-adaptation subsystem should be considered in the earliest stages of establishing the biometric system.

— An administration subsystem, which controls the overall policy, implementation and usage of the biometric system, in accordance with the relevant legal, jurisdictional and societal constraints and privacy requirements. Illustrative examples include:

- provision of privacy relevant information to the subject during biometric processing;
- storage and formatting of the biometric references and/or biometric interchange data;
- making of decisions on encryption and digital signature mechanisms for confidentiality and integrity of PII including biometric data;
- analysis of the vulnerabilities of and security attacks against the overall biometric system and implementation of proper countermeasures;
- provisions of the final arbitration on output from decisions and/or scores;

© ISO/IEC 2011 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24745:2011

- setting of threshold values for the decision subsystem;
- control of the operational environment and non-biometric data storage; and
- provisions of appropriate safeguards for the subject's privacy.

4.3 Biometric references and identity references

A person has one identifier in any particular domain but may have several identity references to identify that person within that domain. Each identity reference is an attribute, or combination of attributes, of the identity of an entity that uniquely identifies that entity in a particular domain. An identity reference can also be a combination of attributes of the person.

A biometric reference is one of many attributes belonging to a person that can be used to recognize that person within a domain. This International Standard classifies identity attributes into non-biometric and biometric ones. For the sake of simplicity, the former is referred to as the identity reference (IR) and the latter as the biometric reference (BR). Some examples, not a comprehensive or definitive list, of identity references and biometric references are depicted in Figure 2. Here, the surrounding box represents the set of attributes that may be used to identify an individual.

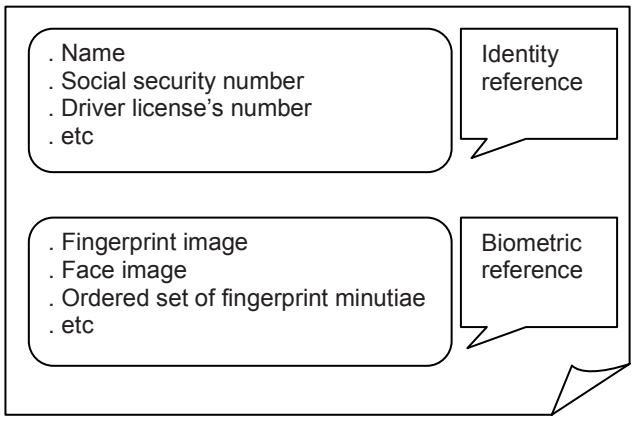

Figure 2 — Identity references and biometric references

4.4 Biometric systems and identity management systems

The identity management system (IdMS) has an important function in any domain to avoid identity conflicts or ambiguities (for more details about IdMS, see ISO/IEC 24760-1). An authentication system requires an accurate identification and verification process, within a well-defined domain, and a defined relationship with registration and enrolment processes which could be in that same domain or called in from another domain. When biometrics is used to provide an authentication service, the IdMS may request authentication from the biometric system (a in Figure 3) and the biometric system may provide the authentication result to the IdMS (b in Figure 3).

© ISO/IEC 2011 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24745:2011

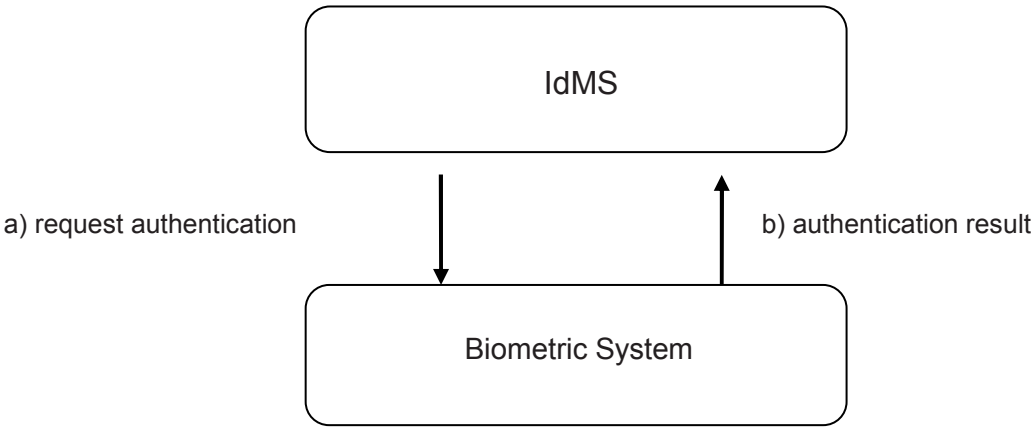

Figure 3 — Biometric system as an authentication service provider for IdMS

4.5 Personally identifiable information and universal unique identifiers

Some biometric systems use biometric samples such as facial images in e-passports to directly identify the person and others use biometric features such as the minutiae points of a fingerprint and the eigenface coefficients of a face to indirectly identify the person bound with the identity reference. This ability to be able to link biometric data to the subject makes biometric references PII.

Due to their distinctiveness, biometric references have the potential to be used as a unique universal identifier (UUID). A UUID is an identity reference which can be used to link personal information across various databases, thereby resulting in a potential threat to privacy. As such, significant concerns have been expressed about using a biometric reference as a UUID. Unless there is a clearly demonstrated need to do so, biometric references should not be used as a universal unique identifier.

The UUID becomes a potential risk to privacy in that an individual can be monitored and tracked across databases containing the corresponding PII. When the biometric reference or its binding with the identity reference is used, it could be classified as personally identifiable information that may be very important to the individual depending on the specific domain [5]. If UUID databases of biometric data are employed, consideration should given to a design that meets requirements for revocability and renewability to limit such cross-comparison, for example, though the use of diversified references as described in this International Standard.

4.6 Societal considerations

The application of biometric systems always has a societal dimension, aspects of which may be codified in legal requirements regarding the operation of such systems (such as those relating to the protection of personal data), while other aspects such as acceptability by subjects using these systems are very desirable and will contribute to good system performance. The acceptability of a system may be influenced by religious, ethnic and cultural factors, as well as by individual psychological traits.

In all deployments of biometric systems those persons and organisations responsible for their operation should recognise that protection of the biometric data by appropriate security mechanisms is necessary to satisfy the legal requirements (for personal data protection), as well as to contribute to their acceptance by society and individuals.

© ISO/IEC 2011 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24745:2011