

BS ISO/IEC 19794-1:2011+A2:2015



BSI Standards Publication

Information technology — Biometric data interchange formats

Part 1: Framework

bsi.

...making excellence a habit.
AVA Documents™
Document Sharing Hub

National foreword

This British Standard is the UK implementation of ISO/IEC 19794-1:2011+A2:2015. It supersedes BS ISO/IEC 19794-1:2011+A1:2013 which is withdrawn.

The start and finish of text introduced or altered by amendment is indicated in the text by tags. Tags indicating changes to ISO/IEC text carry the number of the amendment. For example, text altered by ISO/IEC amendment 1 is indicated in the text by A1 A1.

The UK participation in its preparation was entrusted to Technical Committee IST/44, Biometrics.

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.

© The British Standards Institution 2015.
Published by BSI Standards Limited 2015

ISBN 978 0 580 74907 0

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/corrigenda issued since publication

Date	Text affected
30 April 2013	Implementation of ISO/IEC amendment 1:2013
31 July 2015	Implementation of ISO/IEC amendment 2:2015

Information technology — Biometric data interchange formats —

Part 1: Framework

*Technologies de l'information — Formats d'échange de données
biométriques —*

Partie 1: Cadre



Reference number
ISO/IEC 19794-1:2011(E)

AVA Documents
Document Sharing Hub
© ISO/IEC 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

Contents

Page

Foreword	iv
Introduction	v
1 Scope	1
A1 2 Conformance A1	1
3 Normative references	2
4 Terms and definitions	2
5 Abbreviated terms	11
6 General biometric system	12
6.1 Conceptual diagram of general biometric system	12
6.2 Conceptual components of a general biometric system	12
6.3 Functions of general biometric system	14
7 Usage context of biometric data interchange formats	16
8 General aspects of the usage of biometric data for interchange	16
8.1 Introduction	16
8.2 Natural variability	16
8.3 Aging and usage duration	17
8.4 Enrolment conditions	17
8.5 Feature extraction algorithms	17
8.6 Feature comparison algorithms	17
9 Processing level of data formats for interchange	17
9.1 Processing levels according to ISO/IEC 19785-1	17
9.2 Captured biometric sample	18
9.3 Image data	18
9.4 Behavioural data	18
9.5 Feature data	18
9.6 Naming conventions for biometric data formats	18
9.7 Recommendations for standardizing biometric data formats	19
10 Multibiometrics	19
11 Capture device requirements	19
12 Format owner and format types	20
12.1 Relationship to CBEFF	20
12.2 BDB format owner	21
12.3 BDB format types	21
A2 13 Binary encoding scheme for format types A2	21
13.1 Structure of data records	21
13.2 Common elements for the general header	22
13.3 Common elements for the representation headers	23
A2 14 XML encoding scheme for format types	27
14.1 General	27
14.2 Common elements	30
14.3 Prototypes A2	31
A1 Annex A (normative) Conformance testing methodology A1	32
Annex B (informative) Examples of comparison scenarios	54
A2 Annex C (normative) Common Element XML Schema A2	56
Bibliography	62

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 19794-1 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 37, *Biometrics*.

This second edition cancels and replaces the first edition (ISO/IEC 19794-1:2006), Clause 11 of which has been technically revised. In addition, Clause 3 now includes definitions that are used in multiple parts of ISO/IEC 19794, and Clause 12 has been added to describe general and representation headers that are harmonized across all parts of ISO/IEC 19794.

ISO/IEC 19794 consists of the following parts, under the general title *Information technology — Biometric data interchange formats*:

- *Part 1: Framework*
- *Part 2: Finger minutiae data*
- *Part 3: Finger pattern spectral data*
- *Part 4: Finger image data*
- *Part 5: Face image data*
- *Part 6: Iris image data*
- *Part 7: Signature/sign time series data*
- *Part 8: Finger pattern skeletal data*
- *Part 9: Vascular image data*
- *Part 10: Hand geometry silhouette data*
- *Part 11: Signature/sign processed dynamic data*
- *Part 13: Voice data*
- *Part 14: DNA data*

Introduction

This part of ISO/IEC 19794 defines what is commonly applied for biometric data formats, i.e. the standardization of the common content, meaning, and representation of biometric data formats of biometric modalities considered in the specific parts of ISO/IEC 19794.

Each part of ISO/IEC 19794 can reference text and concepts from documents published by national, international, or industry organizations. Documents from approved reference specification originator (ARO) organizations as defined by JTC 1 will be referenced by citation. Documents from non-ARO organizations can be copied to an annex.

ISO/IEC 19794 is one of a family of International Standards being developed by ISO/IEC JTC 1/SC 37 that support interoperability and data interchange among biometric applications and systems. This family of standards specifies requirements that solve the complexities of applying biometrics to a wide variety of person-recognition applications, whether such applications operate in an open systems environment or consist of a single, closed system. Open systems are built on standards-based, publicly defined data formats, interfaces, and protocols to facilitate data interchange and interoperability with other systems, which can include components of different design or manufacture. A closed system can also be built on publicly defined standards, and can include components of different design or manufacture, but inherently has no requirement for data interchange and interoperability with any other system.

Biometric data interchange format standards and biometric interface standards are both necessary to achieve full data interchange and interoperability for biometric recognition in an open systems environment. The ISO/IEC JTC 1/SC 37 biometric standards family includes a layered set of standards consisting of biometric data interchange formats and biometric interfaces, as well as biometric profiles that describe the use of these standards in specific application areas.

Figure 1 shows the interrelation of biometric-related areas of standardization. Biometric data complying with a biometric data interchange format of ISO/IEC 19794 represents the core component of biometric interoperability. Biometric formats frameworks such as ISO/IEC 19785 (CBEFF) can be used and serve as a wrapper around biometric data. Since biometric data are sensitive data and subject to attack, cryptographic protection is required in interchange environments. Biometric properties with respect to profiles, security evaluation and performance evaluation also play an important role. Biometric interfaces are essential to facilitate easy integration and usage of biometric components. The emerging harmonized vocabulary is recommended for use in describing biometric technology. The deployment of applications using biometric verification or identification takes place within the context of societal and cross-jurisdictional requirements.

The biometric data interchange format standards specify biometric data interchange formats for different biometric modalities. Parties that agree on a biometric data interchange format specified in ISO/IEC 19794 should be able to decode each other's biometric data.

The biometric interface standards include ISO/IEC 19785, *Information technology — Common Biometric Exchange Formats Framework* and ISO/IEC 19784, *Information technology — Biometric application programming interface* (BioAPI). These standards support exchange of biometric data within a system or among systems. ISO/IEC 19785 specifies the basic structure of a standardized Biometric Information Record (BIR), which includes the biometric data interchange record with added metadata such as when it was captured, its expiry date, whether it is encrypted, etc. ISO/IEC 19784 specifies an open system API that supports communications between software applications and underlying biometric technology services.

The biometric profile standards facilitate implementations of the base standards (e.g. the ISO/IEC JTC 1/SC 37 biometric data interchange format and biometric interface standards, and possibly non-biometric standards) for defined applications. These profile standards define the functions of an application (e.g. physical access control for employees at airports) and then specify use of options in the base standards to ensure biometric interoperability.

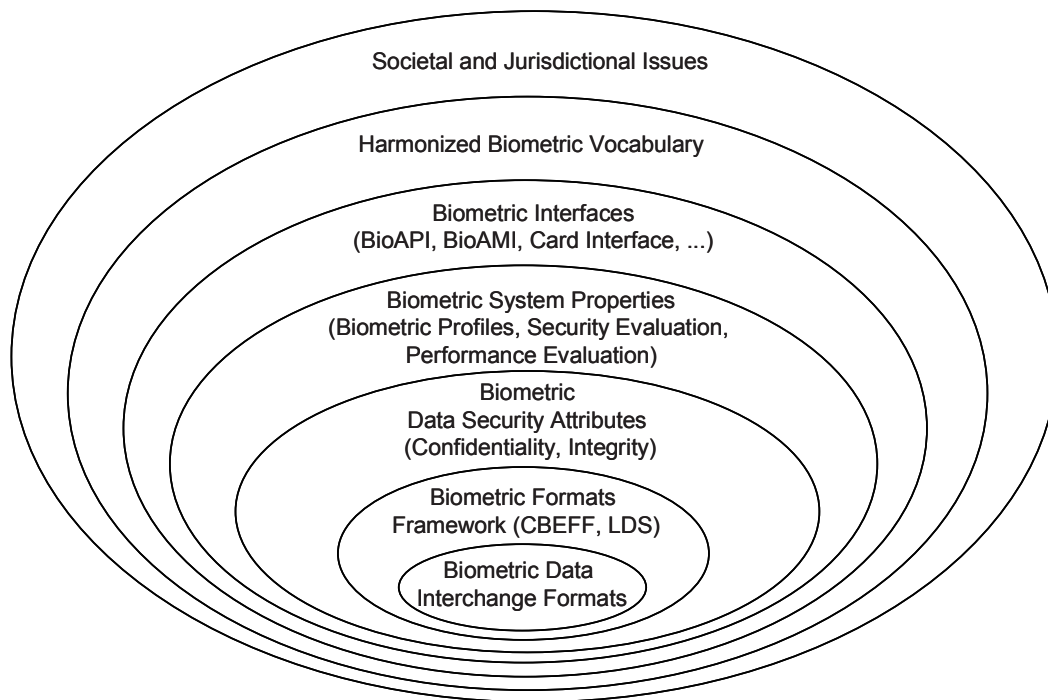


Figure 1 — General interrelation model of biometric issues

A1) Users of biometric systems desire to use this and other standards to ensure that components of the biometric system can be substituted with other components from different vendors with a minimum of effort, and also to ensure that biometric data produced by one system can be used by another system. In order to achieve this, it is critical that systems claimed to conform to a standard actually are conformant, and thus there is a need for a standardized conformance testing methodology for each of the biometric data interchange formats described in ISO/IEC 19794, in order to provide a reasonable degree of assurance that a conformance claim has validity. While conformance of individual elements of data interchange records to relevant requirements can be determined, no test can be absolutely comprehensive and prove that a given system generating or using biometric data interchange records is conformant under all possible circumstances, especially when there are optional components of the standard. A well designed conformance test can, however, test all of the most likely sources of problems and ensure that the implementation under test conforms under a reasonable set of circumstances, giving assurance, but not a guarantee, of conformance.

There are many different types of conformance testing that may be appropriate for the various parts of ISO/IEC 19794. Some of these tests are highly specific to each data interchange format but some of them have many common elements across all of the formats. This part of ISO/IEC 19794 also describes the different types of conformance testing, and provides details of the common elements for defining test assertions. It also provides guidelines for conducting the tests and reporting the results of the tests. Tests and assertions common for most or all biometric data interchange formats (e.g., for common elements of the general headers and the common elements of the representation headers) are specified in this part of ISO/IEC 19794; the specific tests and assertions for each biometric data interchange format are left to the subsequent parts of ISO/IEC 19794.

Annex A of this part of ISO/IEC 19794 is distinct from the ISO/IEC 29109-1 which addressed conformance testing only of the first edition of ISO/IEC 19794. The normative Annex A of this part of ISO/IEC 19794 addresses conformance testing of data formats specified in the second edition of ISO/IEC 19794. **A1)**

Information technology — Biometric data interchange formats —

Part 1: Framework

1 Scope

This part of ISO/IEC 19794 specifies

- general aspects for the usage of biometric data records,
- the processing levels and types of biometric data structures,
- a naming convention for biometric data structures, and
- a coding scheme for format types.

A1 This part of ISO/IEC 19794 also specifies the concepts, test types and conformance testing methodologies to test biometric data interchange records or computer algorithms that create biometric data interchange records. It defines two types (type A, i.e., biometric data interchange records and systems generating such records; and type B, i.e., systems using biometric data interchange records), and three levels (Level 1, i.e., checking internal content of each field; Level 2, i.e., checking internal consistency of the entire record; and Level 3, i.e., checking whether the data record is a faithful representation of the original biometric data) of conformance testing, but it only provides a detailed description and methodology for the three levels of Type A testing. This part of ISO/IEC 19794 specifies test requirements, assertions, and test execution and reporting procedures that are common for most or all biometric data interchange formats. It explicitly does not cover the following areas:

- Modality-specific detailed test elements and assertions or descriptions of any mandatory standard datasets required for testing. They are provided in the subsequent parts of ISO/IEC 19794.
- Testing whether implementations under test (IUTs) that claim to be able to use conformant biometric data interchange records are able to correctly process such biometric data interchange records (Type B testing).
- Conformance testing of CBEFF requirements
- Testing of other characteristics of biometric products or other types of testing of biometric products (i.e., acceptance, performance, robustness, security).

2 Conformance

Biometric data interchange format conformance tests that claim conformance to this part of ISO/IEC 19794 shall satisfy the normative requirements of the methodology for those levels of test they are claiming to perform, as described in Clauses A.1, A.2 and A.3. Any conformance tests shall use the assertion types defined in Clause A.2 with the specific assertion details given in this and the relevant subsequent parts of this standard.

Implementations of subsequent parts of ISO/IEC 19794 tested according to the methodology specified in this part of ISO/IEC 19794 shall be able to claim conformance only to those requirements specified in ISO/IEC 19794 that are tested by the test methods established by this methodology. **A1**

3 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 19785-2, *Information technology — Common Biometric Exchange Formats Framework — Part 2: Procedures for the operation of the Biometric Registration Authority*

ISO/IEC 29794-1:2009, *Information technology — Biometric sample quality — Part 1: Framework*

 RFC 5141, *A Uniform Resource Name (URN) Namespace for the International Organization for Standardization (ISO)*

RFC 5234, *Augmented BNF for Syntax Specifications: ABNF*

XML Schema Part 0: Primer. W3C Recommendation, Second Edition, October 2004 

4 Terms and definitions

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

NOTE Definitions from ISO/IEC 2382-37 and ISO/IEC 2382-29 have been used when available.

4.1

assertion

specification for testing a conformance requirement in an implementation under test expressed in a formal assertion definition language

4.2

assertion test

specification of software or procedural methods that generate the test outcomes used for assessment of conformance to an assertion

NOTE This is adapted from the definition of “assertion test” in ISO/IEC 13210:1999.

4.3

attestation

issue of a statement, based on a decision that fulfillment of specified requirements has been demonstrated

NOTE This is adapted from the definition of “attestation” in ISO/IEC 17000:2004. 

4.4

biometric

of or having to do with **biometrics** (3.2)

NOTE The use of **biometric** as a noun, to mean **biometric** characteristic or **biometric** modality, is deprecated.

EXAMPLE 1 Incorrect usage #1: ICAO resolved that face is the **biometric** most suited to the practicalities of travel documents.

EXAMPLE 2 Correct usage #1: ICAO resolved that face recognition is the **biometric** modality most suited to the practicalities of travel documents.

EXAMPLE 3 Incorrect usage #2: My face **biometric** was encoded in my passport.

EXAMPLE 4 Correct usage #2: My facial **biometric** characteristics were encoded in my passport.

4.5

biometrics

automated recognition of individuals based on their behavioural and biological characteristics

NOTE “Individual” is restricted in scope by ISO/IEC JTC 1/SC 37 to humans.

4.6

biometric algorithm

sequence of instructions that tell a **biometric system** (3.20) how to solve a particular problem

NOTE A **biometric algorithm** will have a finite number of steps and is typically used by the **biometric system** software to decide whether biometric probe data and a biometric reference **match**.

4.7

biometric behavioural data

biometric data (3.7) representing behavioural biometric characteristics of an individual

EXAMPLE Data resulting from writing, speaking, or typing.

4.8

biometric capture device

device that collects a signal from a **biometric characteristic** (3.6) and converts it to a **captured biometric sample** (3.28)

4.9

biometric characteristic

biological and behavioural characteristic of an individual that can be detected and from which distinguishing, repeatable **biometric features** (3.11) can be extracted for the purpose of automated recognition of individuals

4.10

biometric data

biometric sample (3.19) at any stage of processing, **biometric reference** (3.17), **biometric feature** (3.11) or biometric property

EXAMPLE Sensor data, image data, behavioural data, feature data.

4.11

biometric data block

BDB

block of data with a defined format that contains one or more **biometric samples** (3.19) or **biometric templates** (3.21)

NOTE Definition according to CBEFF.

4.12

biometric data interchange record

BDIR

data package containing **biometric data** (3.7) that claims to be in the form prescribed by a base standard

NOTE If the BDIR is encapsulated in a CBEFF record, then the BDIR is also a biometric data block (BDB) as defined in ISO/IEC 19785, but this will not always be the case for BDIRs defined in ISO/IEC 19794.

4.13

biometric data record

data record containing **biometric data** (3.7)

4.14

biometric feature

numbers or labels extracted from **biometric samples** (3.19) and used for **comparison** (3.30)

NOTE 1 Biometric features are the output of a completed **biometric feature extraction**.

NOTE 2 The use of this term needs to be consistent with its use by the pattern recognition and mathematics communities.

NOTE 3 A **biometric feature** set can also be considered a processed **biometric sample**.

4.15

biometric feature data unit

smallest individual unit of extracted feature data

EXAMPLE Minutia of a fingerprint.

4.16

biometric feature extraction

process applied to a **biometric sample** (3.19) with the intent of isolating and outputting repeatable and distinctive numbers or labels which can be compared to those extracted from other **biometric samples** (3.19)

NOTE 1 Filters applied to **biometric samples** (3.19) are not themselves **biometric features** (3.11), however the output of the filter applied to these samples can be. Therefore, for example, eigenfaces are not **biometric features** (3.11).

NOTE 2 Repeatable implies low variation between outputs generated from samples of the same individual.

NOTE 3 Distinctive implies high variation between outputs generated from samples of different individuals.

4.17

biometric image data

pre-processed **biometric data** (3.7) that results from the presentation of an anatomical (i.e. static) **biometric feature** (3.11) of a user and is represented by pixels in a spatial coordinate system

EXAMPLE Fingerprint image data.

4.18

biometric information template

constructed data object in a card containing information needed by the outside world for a verification process

NOTE See ISO/IEC 7816-11.

4.19

biometric model

stored function (dependent on the biometric data subject) generated from one or more **biometric features** (3.11)

4.20

biometric reference

one or more stored **biometric samples** (3.19), **biometric templates** (3.21) or **biometric models** (3.16) attributed to a **biometric data subject** and used for **comparison** (3.30)

EXAMPLE Face image on a passport; fingerprint minutiae template on a national ID card; Gaussian mixture model, for speaker recognition, in a database.

NOTE A biometric reference can be created with implicit or explicit use of auxiliary data, such as Universal Background Models.

4.21

biometric representation

biometric sample (3.19) or biometric feature set

NOTE This term is used in ISO/IEC 19794 for labelling a sub-record in a biometric data interchange record.

4.22

biometric sample

information obtained from a **biometric capture device** (3.5), either directly or after processing

4.23

biometric system

system for the purpose of the automated recognition of individuals based on their behavioural and biological characteristics

4.24

biometric template

reference biometric feature set

set of stored **biometric features** (3.11) comparable directly to **biometric features** (3.11) of a probe **biometric sample** (3.19)

NOTE 1 A **biometric reference** (3.17) consisting of an image, or other **captured biometric sample** (3.28), in its original, enhanced or compressed form, is not a **biometric template** (3.21).

NOTE 2 The **biometric features** (3.11) are not considered to be a **biometric template** (3.21) unless they are stored for reference.

4.25

biometric modality

type of biometric technology

EXAMPLE Fingerprint.

4.26

bit-depth

number of bits used to represent a data element

4.27

byte

contiguous sequence of 8 bits processed as a single unit of information

4.28

candidate

biometric reference identifier of a **biometric reference** (3.17) in the enrolment database determined to be similar to the biometric probe

NOTE Determination can be on the basis of **comparison score** (3.31) and/or rank.

4.29

candidate list

set of zero, one or more **candidates** (3.25) that can be intermediate or final

NOTE Intermediate candidate lists can be produced by systems that use multi-pass biometric identification.

4.30

capture

record or express accurately in words or pictures causing data to be stored in a computer

4.31

captured biometric sample

raw biometric sample (deprecated)

biometric sample (3.19) that is output of biometric capture process

4.32

cell

rectangular region defined by a uniform and non-overlapping division of the image



4.33

certification

third-party attestation related to products

[ISO/IEC 17000:2004]

4.34

comparison

match, noun (deprecated)

matching, noun (deprecated)

estimation, calculation or measurement of similarity or dissimilarity between biometric probe(s) and **biometric reference(s)** (3.17)

NOTE 1 Compare (verb) – “estimate, measure or note the similarity or dissimilarity between”.

NOTE 2 Match (verb) is deprecated as a synonym to compare (verb).

4.35

comparison score

numerical value (or set of values) resulting from a **comparison** (3.30)

4.36

conformance

conformity

fulfillment by a product, process, or service of all relevant specified conformance requirements

NOTE For all practical purposes, data records are considered to be a type of a “product”, i.e., provisions of this standard that are applicable to “products” apply to data records.

4.37

conformance requirement

requirement stated in a data format specification and defined in a finite, measurable, and unambiguous manner

NOTE This is adapted from the definition of “conformance requirement” in ISO/IEC 13210:1999.

4.38

conformance test

specified technical procedure of conformance testing

4.39

conformance testing

testing

determination of one or more characteristics of an object of conformity assessment, according to a procedure

[ISO/IEC 17000:2004]

4.40

conformance testing laboratory

organization that carries out conformance testing.

EXAMPLE This may be the creator of the IUT, the user of the IUT, or an unbiased third party.

4.41

conformance test specification

test specification

provisions of ISO/IEC 19794 biometric data interchange format standard that is concerned with test methods, sometimes supplemented with other provisions related to testing, such as sampling, use of statistical methods, and sequence of tests

NOTE This is adapted from the definition of “testing standard” in ISO/IEC GUIDE 2:2004.

4.42

conformance testing suite

CTS

test software used to automate certain types of conformance testing 

A1 4.43

conformity assessment

demonstration that specified requirements relating to a product, process, system, person or body are fulfilled

[ISO/IEC 17000:2004] **A1**

4.44

continuous tone image

image whose components have more than one bit per **pixel** (3.45)

4.45

core

topmost point on the innermost recurving ridgeline of a fingerprint

NOTE Generally, the core is placed upon or within the innermost recurve of a loop.

A1 4.46

data format specification

provisions of ISO/IEC 19794 biometric data interchange format standard containing the specification that is the subject of the conformance testing

4.47

declaration

declaration of conformity first-party attestation

[ISO/IEC 17000:2004] **A1**

4.48

delta

point on a ridge at or nearest to the point of divergence of two **typelines** (3.56) and located at or directly in front of the point of divergence

4.49

dimension

number of pixels in a **captured biometric sample** (3.28) either in x- or y-direction

4.50

enrolment

registration (deprecated)

process of creating and storing, for an individual, a data record associated with an individual and including **biometric reference(s)** (3.17) and, typically, non-biometric data

4.51

friction ridge

ridge present on the skin of the fingers and toes, the palms and soles of the feet, which makes contact with an incident surface under normal touch

NOTE On the fingers, the unique patterns formed by the friction ridges make up fingerprints.

4.52

identification

⟨biometric system function⟩ biometric system function that performs a one-to-many search to obtain a candidate list

EXAMPLE BioAPI_IdentifyMatch.

NOTE An identification function can be used to verify a claim of **enrolment** (3.36) in an enrolment database without a specified biometric reference identifier.

A1 4.53

Implementation conformance statement

ICS

statement by the supplier of an implementation under test that indicates which mandatory and optional components of the data format specification are supported by the implementation

4.54

implementation under test

IUT

that which implements the data format specification being tested

NOTE Depending on the conformance requirements of the data format specification, this may simply be a set of biometric data interchange records or it may be a computer algorithm in the form that creates the BDIR and/or uses the data contained in the BDIR.

4.55

input biometric data record

IBDR

data package containing a less processed form of biometric data which is suitable for use in the creation of a BDIR

NOTE In some cases, this may be an image, but it may also be raw sensor output such as a time series of data points from a digitization tablet. **A1**

4.56

intermediate biometric sample

biometric sample (3.19) following intermediate biometric sample processing

EXAMPLE Intermediate biometric samples might have been enhanced for **biometric feature** (3.11) extraction, compressed for compact storage purposes, etc.

4.57

latent fingerprint

impression of a fingerprint image collected from an intermediate surface, rather than directly via a live scan capture device or a traditional inked fingerprint card

A1 4.58

level 1 testing

conformance testing methodology that checks field by field and byte by byte conformance with the specification of the BDIR as specified in the data format specification, both in terms of fields included and the ranges of the values in those fields

NOTE This type of testing tests syntactic requirements of the data format specification.

4.59

level 2 testing

conformance testing methodology that tests the internal consistency of the BDIR under test, relating values from one part or field of the BDIR to values from other parts or fields of the BDIR

NOTE This type of testing tests syntactic requirements of the data format specification.

4.60

level 3 testing

conformance testing methodology that tests that a BDIR produced by an IUT is a faithful representation of the IBDR subject to the constraints of the parameters in the metadata records

NOTE This type of testing tests semantic requirements of the data format specification. **A1**

4.61

live capture

process of capturing a **biometric sample** (3.19) through an interaction between an end user and a biometric system

A1 4.62

metadata record

data record containing any specific parameters related to the data itself, particularly required by an IUT to transform an IBDR into a BDIR

EXAMPLE Type of image (basic, full frontal, token frontal or other) and the level of compression for a face image BDIR; the presence of core, delta, or ridgecounts in the extended area for finger minutiae BDIR; the size of each pattern in a finger pattern BDIR. **A1**

4.63

minutia

friction ridge characteristic that is used to individualize a fingerprint

NOTE 1 The plural is “minutiae”.

NOTE 2 Minutiae occur at points where a single friction ridge deviates from an uninterrupted flow. Deviation may take the form of ending, bifurcation, or a more complicated “composite” type.

4.64

multipresentation

using either multiple presentation samples of one instance of a biometric characteristic or a single presentation that results in the capture of multiple samples

EXAMPLE Several frames from video camera capture of a face image (possibly but not necessarily consecutive).

NOTE Multipresentation biometrics is considered a form of multibiometrics, if fusion techniques are employed.

4.65

multisensorial

using multiple sensors for capturing samples of one biometric instance

4.66

pixel

picture element

point in an image that is represented by an n-by-m matrix of points, where n is the number of horizontal rows and m is the number of vertical columns,

4.67

pixel depth

number of bits used to represent the luminance and/or chrominance value of a pixel

A1 4.68

procedure

specified way to carry out an activity or a process

[ISO 9000:2005] **A1**

4.69

raw

image file in which the image is stored in the same format in which it is stored in video memory, typically one byte (for monochrome images) per **pixel** (3.45) or three bytes (for colour images) per **pixel** (3.45)

A1 4.70

requirement

provision that conveys criteria to be fulfilled

[ISO/IEC GUIDE 2:2004] **A1**

4.71

ridge bifurcation

minutia assigned to the location at which a friction ridge splits into two ridges or, alternatively, where two separate friction ridges combine into one

4.72

ridge ending

minutia assigned to the location at which a friction ridge terminates or, alternatively, begins

NOTE A ridge ending corresponds to the bifurcation of the adjacent valley: the location at which a valley splits into two valleys or, alternatively, at which two separate valleys combine into one.

4.73

signature/sign

handwritten signature or handwritten personal sign

4.74

skeleton

one-pixel-wide representation of the topology of an object

NOTE The skeleton is also known as the medial axis.

4.75

spatial sampling rate

resolution (deprecated)

number of **pixels** (3.45) per unit distance in the object space, specified as the number of pixels per millimetre in the object space along the applicable coordinate axes

4.76

swipe fingerprint image

method of fingerprint collection where the finger is manually slid across a one-dimensional sensor resulting in multiple readings or partial impressions from the same fingerprint

NOTE These readings are then combined to produce an accurate two-dimensional image of the fingerprint.

4.77

test method

specified technical procedure for performing a test

NOTE This is adapted from the definition of “test method” in ISO/IEC GUIDE 2:1996. More recent edition of ISO/IEC GUIDE 2 or ISO/IEC 17000:2004 no longer contain this definition

4.78

test report

document that presents test results and other information relevant to the execution of the test methods against an Implementation Under Test

NOTE This is adapted from the definition of “test report” in ISO/IEC 13210:1999 and ISO/IEC GUIDE 2:1996. 

4.79

time series

sequence of values sampled at successive points in time

4.80

transaction

sequence of attempts on the part of a user for the purposes of an enrolment, verification or identification

A1 4.81

Type A conformance claim

conformance claim that an IUT is a conformant BDIR, or can create conformant BDIRs from appropriate IBDRs

4.82

Type B conformance claim

conformance claim that an IUT can read conformant BDIRs, interpret them correctly, and perform its desired function upon them **A1**

4.83

typeline

one of the two innermost **friction ridges** (3.37) that start parallel, diverge, and surround or tend to surround the pattern area

4.84

user

⟨biometric system⟩ person or organization interacting in any way with a biometric system

4.85

valley

area between two **friction ridges** (3.37) that does not make contact with an incident surface under normal touch

4.86

verification

authentication (deprecated)

positive identification (deprecated)

⟨biometric system function⟩ biometric system function that performs a one-to-one **comparison** (3.30)

EXAMPLE BioAPI_VerifyMatch.

NOTE An identification application can use an exhaustive series of verification function calls.

5 Abbreviated terms

For the purposes of this document, the following abbreviated terms apply.

A2	ABNF	Augmented BNF for Syntax Specifications A2
	API	Application Programming Interface
	BDB	Biometric Data Block
	BDIR	Biometric Data Interchange Record
	BIR	Biometric Information Record
	CBEFF	Common Biometric Exchange Formats Framework
A1	CTS	Conformance Testing Suite A1
	IBIA	International Biometric Industry Association
A1	IBDR	Input Biometric Data Record
	ICS	Implementation Conformance Statement
	IUT	Implementation Under Test A1
	LDS	Logical Data Structure
	SB	Security Block
	SBH	Standard Biometric Header
A2	XML	Extensible Markup Language A2

6 General biometric system

6.1 Conceptual diagram of general biometric system

Given the variety of applications and technologies, it might seem difficult to draw any generalizations about biometric systems. All such systems, however, have many elements in common. Captured biometric samples are acquired from a subject by a biometric capture device. The biometric capture device output may be sent to a processor that extracts the distinctive but repeatable measures of the sample (the “features”), discarding all other components. The resulting features can be stored in the database as a “reference”, sometimes called a “biometric reference” or a biometric “template”. In other cases the sample (without feature extraction) may be stored as the biometric reference. A new sample can be compared to a specific reference, to many references or all references already in the database to determine if there is a match. A decision regarding the identity claim is made based upon the similarities or dissimilarities between the sample features and those of the reference or references compared.

Figure 2 illustrates the information flow within a general biometric system, showing a general biometric system consisting of data capture, signal processing, storage, comparison and decision subsystems. This diagram illustrates both enrolment, and the operation of verification and identification systems. The following sub-clauses describe each of these subsystems in more detail.

NOTE In any implemented system, some of these conceptual components may be absent or may not have a direct correspondence with a physical or software entity.

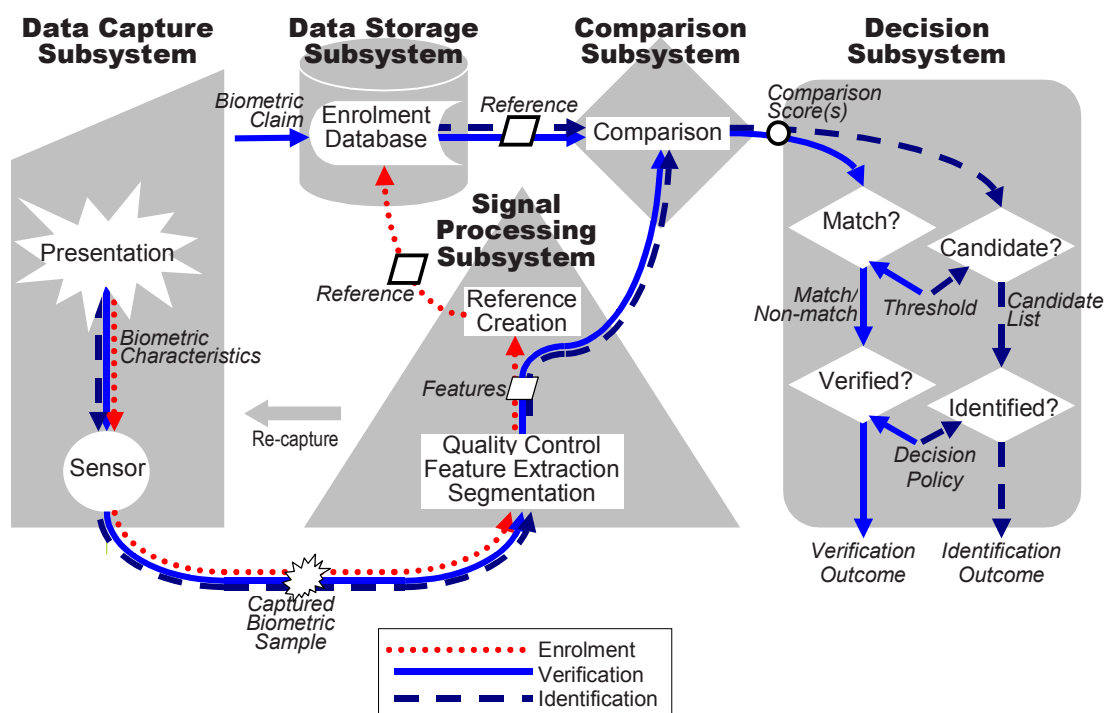


Figure 2 — Components of a general biometric system

6.2 Conceptual components of a general biometric system

6.2.1 Data capture subsystem

The data capture subsystem collects an image or signal of a subject's *biometric characteristics* that they have *presented* to the biometric capture device, and outputs this image/signal as a *captured biometric sample*.

NOTE In Clause 5, italics are used for components shown in Figure 2.

6.2.2 Transmission subsystem

The transmission subsystem (not portrayed in diagram; not always present or visibly present in a biometric system) will transmit *samples*, *features*, and/or *references* between different subsystems. *Samples*, *features* or *references* may be transmitted using standard biometric data interchange formats. The captured *biometric sample* may be compressed and/or encrypted before transmission, and expanded and/or decrypted before use. A captured *biometric sample* may be altered in transmission due to noise in the transmission channel as well as losses in the compression/expansion process. It is advisable that cryptographic techniques be used to protect the authenticity, integrity, and confidentiality of stored and transmitted biometric data.

6.2.3 Signal processing subsystem

Signal processing may include processes such as

- *segmentation*, i.e. locating the signal of the subject's biometric characteristics within the captured biometric sample,
- *feature extraction*, i.e. deriving the subject's repeatable and distinctive measures from the captured biometric sample,
- *quality control*, i.e., assessing the suitability of samples, features, references, etc. and possibly affecting other processes, such as returning control to the data capture subsystem to collect further *samples*; or modifying parameters for segmentation, feature extraction, or comparison,
- *image enhancement*, i.e. improving the quality and clarity of the captured biometric sample.

In the case of enrolment, the signal processing subsystem creates a reference. Sometimes the enrolment process requires features from several presentations of the individual's biometric characteristics. Sometimes the *reference* comprises just the *features*, in which case the reference may be called a "template". Sometimes the reference comprises just the sample, in which case feature extraction from the reference may occur immediately before comparison.

Sequencing and iteration of the above-mentioned processes are determined by the specifics of each system.

6.2.4 Data storage subsystem

References are stored within an *enrolment database* held in the data storage subsystem. Each *reference* might be associated with some details of the enrolled subject or the enrolment process. It should be noted that prior to being stored in the *enrolment database*, *references* may be re-formatted into a biometric data interchange format. *References* may be stored within a biometric capture device, on a portable medium such as a smart card, locally such as on a personal computer or local server, or remotely in a central database.

6.2.5 Comparison subsystem

In the comparison subsystem, the *features* are compared against one or more *references* and *comparison scores* are passed to the decision subsystem. The *comparison scores* indicate the similarities or dissimilarities between the *features* and *reference/s* compared. In some cases, the *features* may take the same form as the stored *reference*. For verification, a single specific claim of subject enrolment would lead to a single *comparison score*. For identification, many or all *references* may be compared with the *features*, and a *comparison score* may be produced for each comparison.

6.2.6 Decision subsystem

The decision subsystem uses the *comparison scores* generated from one or more attempts to provide the decision *outcome* for a verification or identification transaction.

In the case of verification, the *features* are considered to *match* a compared *reference* when (assuming that higher scores correspond to greater similarity) the *comparison score* exceeds a specified *threshold*. A claim about the subject's enrolment can then be verified on the basis of the *decision policy*, which may allow or require multiple attempts.

In the case of identification, an enrollee reference is a potential *candidate* for the subject when (assuming that higher scores correspond to greater similarity) the *comparison score* exceeds a specified *threshold*, and/or when the *comparison score* is among the highest ranked values generated during comparisons across the entire database. The *decision policy* may allow or require multiple attempts before making an identification decision.

NOTE Conceptually, it is possible to treat multibiometric systems in the same manner as unibiometric systems, by treating the combined captured biometric *samples/references/scores* as if they were a single *sample/reference/score* and allowing the decision subsystem to operate score fusion or decision fusion as and if appropriate. (See also ISO/IEC TR 24722:2007 Multimodal and other multibiometric fusion).

6.2.7 Administration subsystem

The administration subsystem (not portrayed in diagram) governs the overall policy, implementation and usage of the biometric system, in accordance with the relevant legal, jurisdictional and societal constraints and requirements. Illustrative examples include:

- requesting additional information from the subject,
- providing final arbitration on output from decision and/or scores,
- setting *threshold* values for decision,
- setting biometric system acquisition settings,
- controlling the operational environment and non-biometric data storage,
- providing appropriate safeguards for subject privacy,
- interacting with the application that utilizes the biometric system,
- defining decision criteria for *verification* or *identification*.

6.2.8 Interface

The biometric system may or may not interface to an external application or system via an Application Programming Interface, Hardware Interface or Protocol Interface (not portrayed in diagram).

6.3 Functions of general biometric system

6.3.1 Enrolment

In enrolment, a transaction by a subject is processed by the system in order to generate and store an enrolment reference for that individual.

Enrolment typically involves:

- sample acquisition,
- segmentation,
- feature extraction,

- quality checks (which may reject the sample/features as being unsuitable for creating a reference, and require acquisition of further samples),
- biometric reference creation (which may require features from multiple samples), possible conversion into a biometric data interchange format and storage,
- test verification or identification attempts to ensure that the resulting enrolment is usable, and
- allowing repeat enrolment attempts, should the initial enrolment be deemed unsatisfactory (dependent on the enrolment policy).

6.3.2 Verification

In verification, a transaction by a subject is processed by the system in order to verify a positive specific claim about the subject's enrolment (e.g. "I am enrolled as subject X"). The verification function will either accept or reject the claim. The verification decision outcome is considered to be erroneous if either a false claim is accepted (false accept) or a true claim is rejected (false reject).

NOTE Some biometric systems will allow a single subject to enrol more than one instance of a biometric characteristic (for example, an iris system may allow subjects to enrol both iris images, while a fingerprint system may require enrolment of additional fingers for fallback in case a primary finger is damaged).

Verification typically involves:

- signal processing,
- sample acquisition,
- segmentation,
- feature extraction,
- quality checks (which may reject the sample/features as being unsuitable for comparison, and require acquisition of further samples),
- comparison of the sample features against the reference for the claimed identity producing a comparison score,
- determination of whether the sample features match the reference based on whether the comparison score exceeds a threshold (assuming that higher scores correspond to greater similarity), and
- decision to verify based on the comparison result of one or more attempts as dictated by the decision policy.

EXAMPLE In a verification system allowing up to three attempts to be matched to an enrolled reference, a false rejection will result with any combination of failures-to-acquire and false non-matches over three attempts. A false acceptance will result if a sample is acquired and falsely matched to the enrolled reference for the claimed identity on any of three attempts.

6.3.3 Identification

In identification, a *transaction* by a subject is processed by the system and the enrolment database is searched to find matching references. Identification provides a *candidate list* of identifiers that will contain zero, one, or more identifiers. Identification is considered correct when the subject is enrolled, and an identifier for their enrolment is in the candidate list. The identification is considered to be erroneous if either an enrolled subject's identifier is not in the resulting candidate list (false-negative identification error), or if a transaction by a non-enrolled subject produces a non-empty candidate list (false-positive identification error).