INTERNATIONAL STANDARD

ISO/IEC 19794-1

Second edition
2011-07-15

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)

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

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.

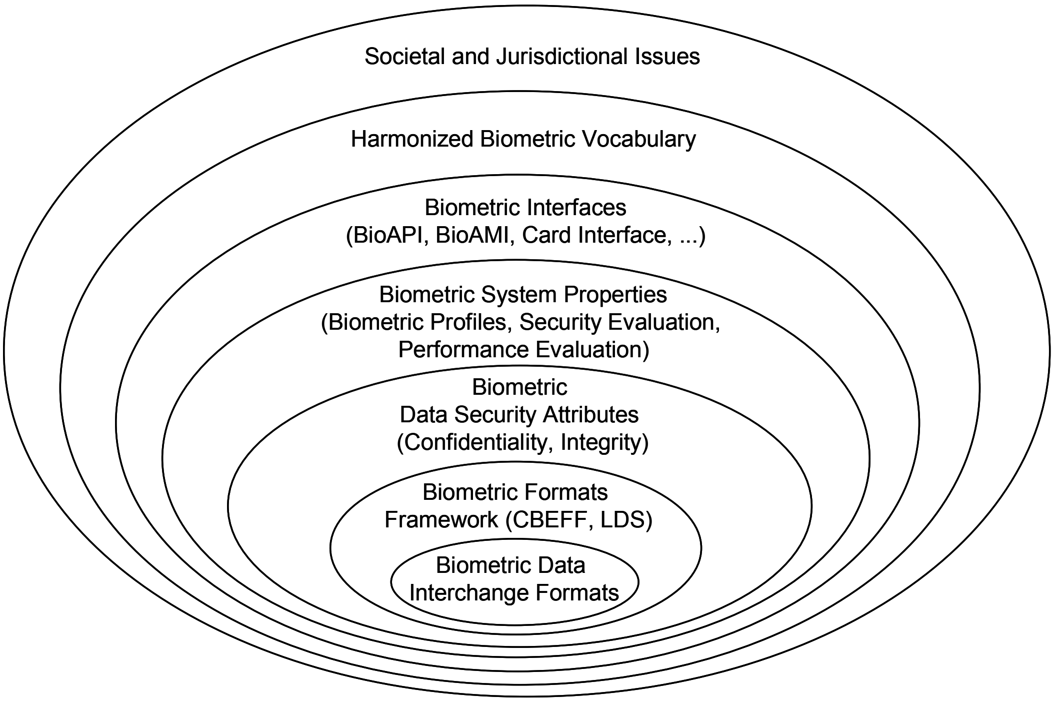
Societal and Jurisdictional Issues
Harmonized Biometric Vocabulary
Biometric Interfaces
(BioAPI, BioAMI, Card Interface, ...)
Biometric System Properties
(Biometric Profiles, Security Evaluation,
Performance Evaluation)
Biometric
Data Security Attributes
(Confidentiality, Integrity)
Biometric Formats
Framework (CBEFF, LDS)
Biometric Data
Interchange Formats

Figure 1 — General interrelation model of biometric issues

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.

2 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*

3 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.

3.1
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.

3.2
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.

3.3
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**.

3.4
biometric behavioural data
biometric data (3.7) representing behavioural biometric characteristics of an individual

EXAMPLE Data resulting from writing, speaking, or typing.

3.5
biometric capture device
device that collects a signal from a **biometric characteristic** (3.6) and converts it to a **captured biometric sample** (3.28)

3.6
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

3.7
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.

3.8
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.

3.9
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.

3.10
biometric data record
data record containing **biometric data** (3.7)

3.11
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**.

3.12
biometric feature data unit
smallest individual unit of extracted feature data

EXAMPLE Minutia of a fingerprint.

3.13
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.

3.14
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.

3.15
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.

3.16
biometric model
stored function (dependent on the biometric data subject) generated from one or more **biometric features** (3.11)

3.17
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.

3.18
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.

3.19
biometric sample
information obtained from a **biometric capture device** (3.5), either directly or after processing

3.20
biometric system
system for the purpose of the automated recognition of individuals based on their behavioural and biological characteristics

3.21
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.

3.22
biometric modality
type of biometric technology

EXAMPLE Fingerprint.

3.23
bit-depth
number of bits used to represent a data element

3.24
byte
contiguous sequence of 8 bits processed as a single unit of information

3.25
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.

3.26
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.

3.27
capture
record or express accurately in words or pictures causing data to be stored in a computer

3.28
captured biometric sample
raw biometric sample (deprecated)
biometric sample (3.19) that is output of biometric capture process

3.29
cell
rectangular region defined by a uniform and non-overlapping division of the image

3.30
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).

3.31
comparison score
numerical value (or set of values) resulting from a **comparison** (3.30)

3.32
continuous tone image
image whose components have more than one bit per **pixel** (3.45)

3.33
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.

3.34
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

3.35
dimension
number of pixels in a **captured biometric sample** (3.28) either in x- or y-direction

3.36
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

3.37
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.

3.38
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.

3.39
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.

3.40
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

3.41
live capture
process of capturing a **biometric sample** (3.19) through an interaction between an end user and a biometric system

3.42
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.

3.43
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.

3.44
multisensorial
using multiple sensors for capturing samples of one biometric instance

3.45
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,

3.46
pixel depth
number of bits used to represent the luminance and/or chrominance value of a pixel