INTERNATIONAL STANDARD

ISO/IEC 19794-1

First edition
2006-04-01

Information technology — Biometric data interchange formats —

Part 1: Framework

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

Partie 1: Cadre général

Reference number
ISO/IEC 19794-1:2006(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*.

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*

The following part is under preparation:

— *Part 11: Signature/sign processed dynamic data*

Introduction

This part of ISO/IEC 19794 is intended to describe the general aspects and requirements for defining biometric data interchange formats.

The notation and transfer formats provide platform independence and separation of transfer syntax from content definition. 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 types considered in the specific parts of ISO/IEC 19794.

Figure 1 shows the interrelation of biometric-related ISO/IEC standardization fields. Biometric data complying with a biometric data interchange format of ISO/IEC 19794 represent the core component of biometric interoperability. Biometric formats frameworks such as ISO/IEC 19785 (CBEFF) 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 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.

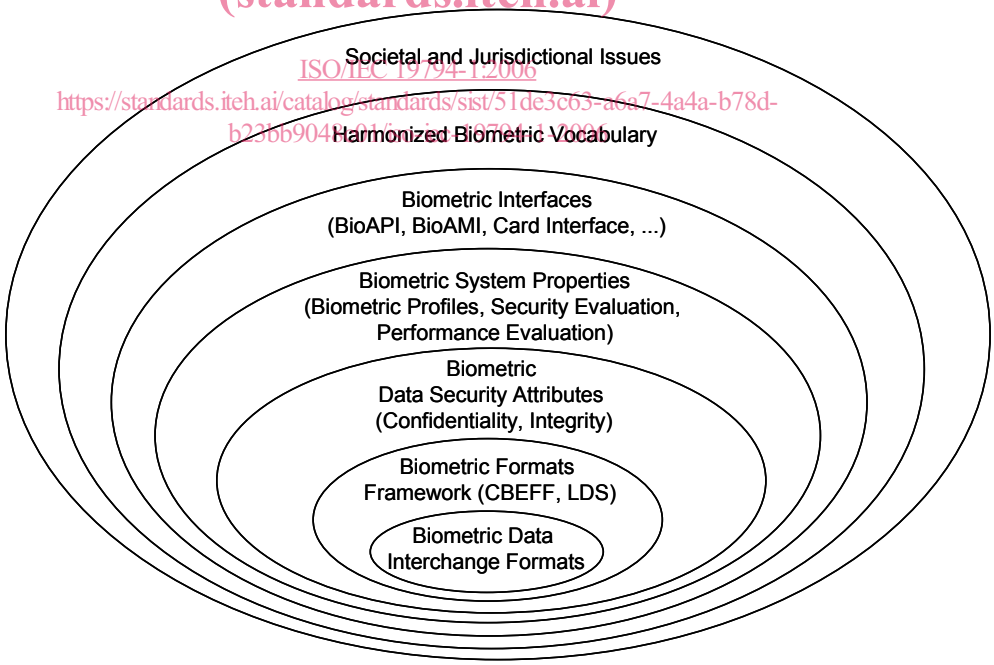

Figure 1 — General interrelation model of biometric issues

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 structures,

— the types of biometric data structure,

— a naming concept for biometric data structures,

— a coding scheme for format types.

Biometric data include but are not limited to finger minutiae, finger pattern, finger image, face image, iris image and signature/sign behavioural data.

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 7816-11:2004, *Identification cards – Integrated circuit cards – Part 11: Personal verification through biometric methods*

ISO/IEC 19785-1:—, *Information technology – Common Biometric Exchange Formats Framework – Part 1: Data element specification* [1]

ISO/IEC 19785-3:—, *Information technology – Common Biometric Exchange Formats Framework – Part 3: Patron format specifications* [1]

3 Terms and definitions

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

3.1
biometric
pertaining to the field of biometrics

[1] To be published.

3.2
biometrics
automated recognition of living persons based on observation of behavioural and biological (anatomical and physiological) characteristics

3.3
biometric algorithm
sequence of instructions that tell a biometric system 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 verification or identification data and a biometric template match.

3.4
biometric behavioural data
biometric data resulting from a dynamic action of the user

EXAMPLE data resulting from writing, speaking, or typing

3.5
biometric data
any data representing a biometric characteristic

EXAMPLE sensor data, image data, behavioural data, feature data

3.6
biometric feature
representation of a biometric characteristic that can be used by a biometric algorithm for the purpose of comparing data sets of the same biometric type with each other

NOTE The biometric feature may be composed of individual biometric feature data units.

3.7
biometric feature data unit
smallest individual unit of extracted feature data

EXAMPLE minutia of a fingerprint

3.8
biometric feature extraction
process of converting pre-processed sensor data into a biometric template, verification or identification data so that it can be compared with other extracted feature data

3.9
biometric identification
one-to-many process of comparing submitted biometric data against all records of a database to determine whether it matches and, if so, to identify the respective person

3.10
biometric identification data
data acquired during an identification process for comparison with several biometric templates

3.11
biometric image data
pre-processed biometric data that result from the presentation of a physiological (i.e. static) biometric feature of a user and are represented by pixels in a spatial coordinate system

EXAMPLE fingerprint image data

3.12
biometric information
information needed by the feature extraction and data formatting components of a biometric system to construct the biometric verification or identification data

3.13
biometric template
biometric sample or combination of biometric samples that is suitable for storage as a reference for future comparison

3.14
biometric sample
information obtained from a biometric device, either directly or after processing

3.15
biometric system
automated system capable of capturing biometric sensor data from a user, extracting feature data from that processed acquired data, comparing the processed feature data with those contained in one or more biometric templates, deciding how well they match, and indicating whether or not an identification or verification of identity has been achieved

3.16
biometric type
type of biometric technology

EXAMPLE fingerprint

3.17
biometric verification
automated process of assessing a claim that submitted biometric sample(s) and a stored biometric template are from the same source

3.18
biometric verification data
data acquired during a verification process for comparison with the biometric template

3.19
enrolment
process of collecting biometric data from a person and the subsequent preparation and storage of biometric templates representing that person's identity

3.20
intermediate biometric sample
biometric sample obtained by processing an acquired biometric sample, intended for further processing

3.21
matching
process of comparing biometric data with a previously stored biometric template and scoring the level of similarity

NOTE An accept or reject decision is then based on whether this score exceeds the given threshold.

3.22
processed biometric sample
biometric sample suitable for comparison

3.23
acquired biometric sample
raw biometric sample
biometric sample obtained directly from an individual by means of a biometric capture device

4 Abbreviated terms

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

API	Application Programming Interface
BDB	Biometric Data Block
CBEFF	Common Biometric Exchange Formats Framework
IBIA	International Biometric Industry Association
LDS	Logical Data Structure
SB	Signature Block
SBH	Standard Biometric Header

5 General biometric system

5.1 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. Biometric samples are acquired from a subject by a sensor. The sensor output is sent to a processor which 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 "template", or compared to a specific template, many templates or all templates already in the database to determine if there is a match. A decision regarding the identity claim is made based upon the similarity between the sample features and those of the template or templates compared.

Figure 2 illustrates the information flow within a general biometric system, showing a general biometric system consisting of data capture, signal processing, storage, matching and decision subsystems. This diagram

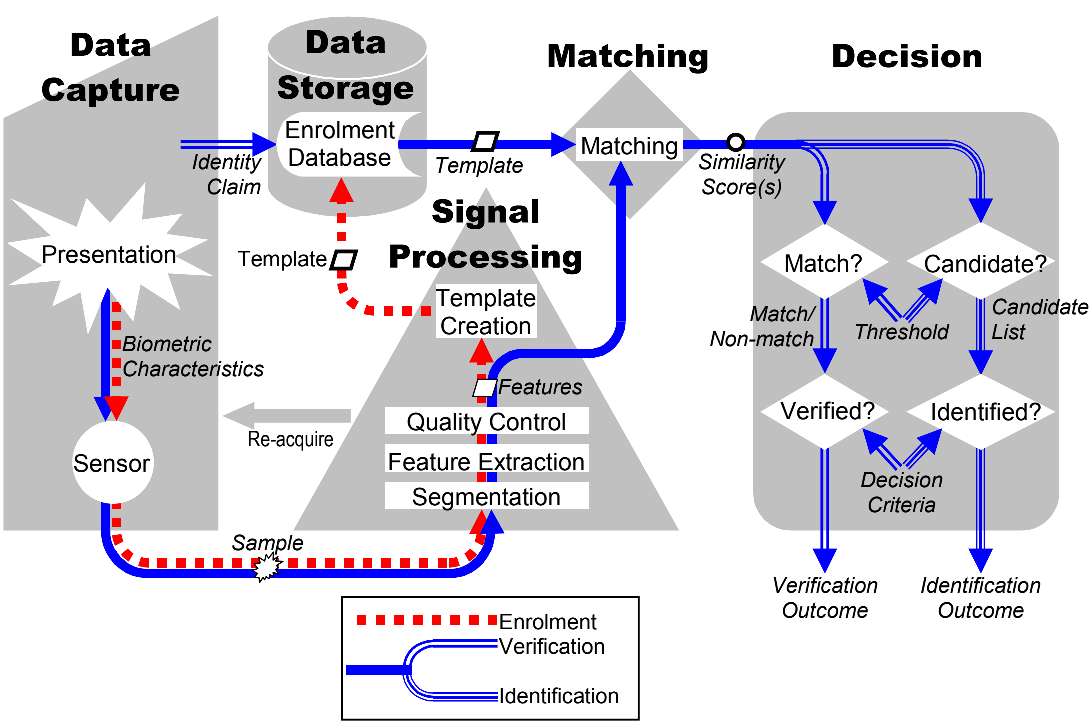

Figure 2 — Components of general biometric system

illustrates both enrolment, and the operation of verification and identification systems. The following subclauses describe each of these subsystems in more detail. It should be noted that, in any real biometric system, these conceptual components may not exist or may not directly correspond to the physical components.

5.2 Conceptual components of a general biometric system

5.2.1 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 sensor*, and outputs this image/signal as a *biometric sample*.

5.2.2 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 *templates* between different subsystems. *Samples, features* or *templates* may be transmitted using standard biometric data interchange formats. The biometric *sample* may be compressed and/or encrypted before transmission, and expanded and/or decrypted before use. A 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.

5.2.3 Signal processing subsystem

The signal processing subsystem extracts the distinguishing *features* from a biometric *sample*. This may involve locating the signal of the subject's *biometric characteristics* within the received *sample* (a process known as *segmentation*), *feature extraction*, and *quality control* to ensure that the extracted features are likely to be distinguishing and repeatable. Should *quality control* reject the received *sample/s*, control may return to the data capture subsystem to collect a further *sample/s*.

In the case of enrolment, the signal processing subsystem creates a *template* from the extracted biometric *features*. Often the enrolment process requires *features* from several presentations of the individual's *biometric characteristics*. Sometimes the *template* comprises just the *features*.

5.2.4 Data storage subsystem

Templates are stored within an *enrolment database* held in the data storage subsystem. Each *template* is associated with details of the enrolled subject. It should be noted that prior to being stored in the *enrolment database*, *templates* may be re-formatted into a biometric data interchange format. *Templates* 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 in a central database.

5.2.5 Matching subsystem

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

5.2.6 Decision subsystem

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