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.

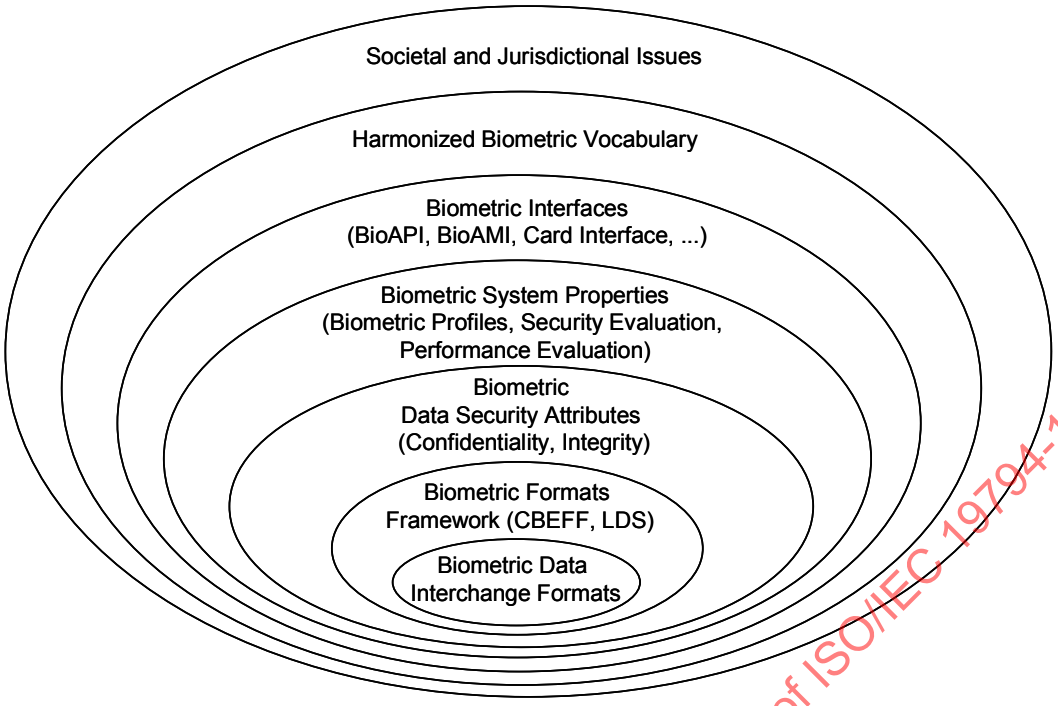

Figure 1 — General interrelation model of biometric issues

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

3.47
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)

3.48
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

3.49
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.

3.50
signature/sign
handwritten signature or handwritten personal sign

3.51
skeleton
one-pixel-wide representation of the topology of an object

NOTE The skeleton is also known as the medial axis.

3.52
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

3.53
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.

3.54
time series
sequence of values sampled at successive points in time

3.55
transaction
sequence of attempts on the part of a user for the purposes of an enrolment, verification or identification

3.56
typeline
one of the two innermost **friction ridges** (3.37) that start parallel, diverge, and surround or tend to surround the pattern area

3.57
user
⟨biometric system⟩ person or organization interacting in any way with a biometric system

3.58
valley
area between two **friction ridges** (3.37) that does not make contact with an incident surface under normal touch

3.59
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.

4 Abbreviated terms

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

API	Application Programming Interface
BDB	Biometric Data Block
BDIR	Biometric Data Interchange Record
BIR	Biometric Information Record
CBEFF	Common Biometric Exchange Formats Framework
IBIA	International Biometric Industry Association
LDS	Logical Data Structure
SB	Security 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. 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.

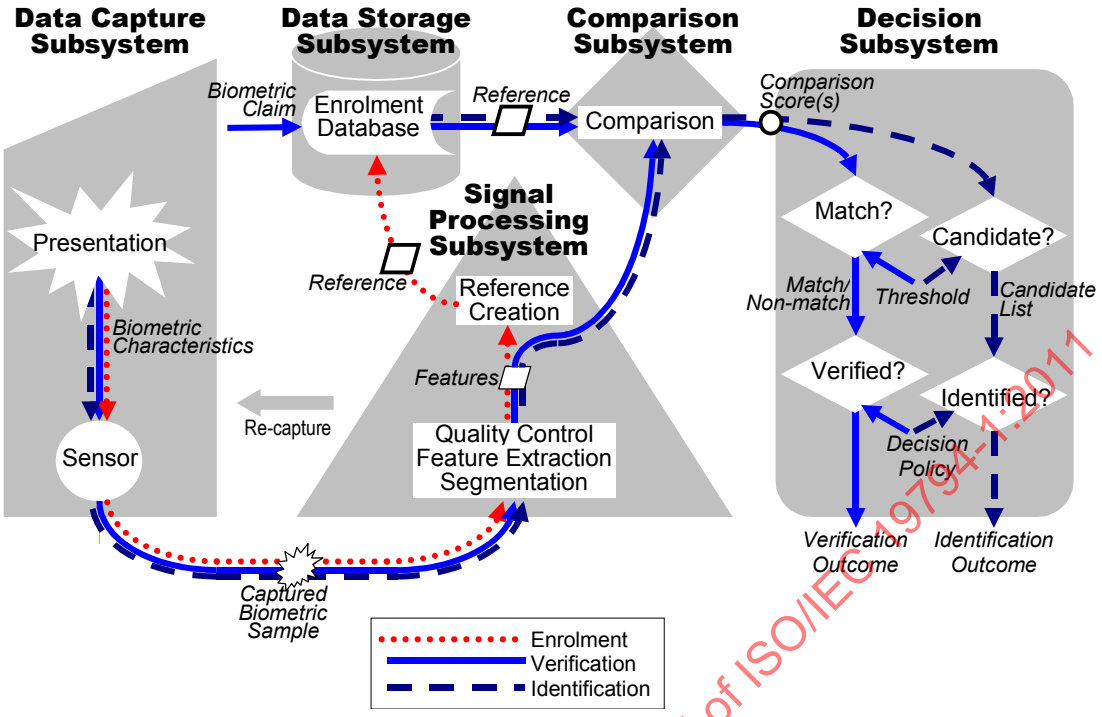

Figure 2 — Components of a general biometric system

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 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.

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 *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.

5.2.3 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.

5.2.4 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.

5.2.5 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.

5.2.6 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 enrolee 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).

5.2.7 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*.

5.2.8 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).

5.3 Functions of general biometric system

5.3.1 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).

5.3.2 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.

5.3.3 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).

Identification 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 against some or all references in the enrolment database, producing a comparison score for each comparison,

— determination of whether each compared reference is a potential candidate identifier for the user, based on whether the comparison score exceeds a threshold and/or is among the highest ranked scores returned, producing a candidate list (assuming that higher scores correspond to greater similarity), and

— an identification decision based on the candidate lists from one or more attempts, as dictated by the decision policy.

6 Usage context of biometric data interchange formats

The structure and content of biometric data records for interchange depend on the intended usage context. There may be

— self-contained data structures providing all necessary information,

— data structures designed for the biometric data block of CBEFF not duplicating information which is present in the CBEFF standard biometric header,

— data structures for usage in a Biometric Information Template as defined in ISO/IEC 7816-11 and ISO/IEC 19785-3,

— data structures designed for on-card biometric comparison as defined in ISO/IEC 24787.

7 General aspects of the usage of biometric data for interchange

7.1 Introduction

When using biometric data, the general aspects specified in the following clauses should be taken into consideration.

7.2 Natural variability

Biometric samples and reference data from the same person do not generally result in a perfect match when performing a comparison. A person may never be able to present exactly the same data again since they depend on a lot of factors where smallest changes (e.g. translation, rotation and distortion of fingers) already result in different data. Therefore it may be necessary to specify, together with the biometric data structure, specific parameters such as tolerances for the range of presentation parameters that may be acceptable.

7.3 Aging and usage duration

Some biometric characteristics (e.g. facial image or signature dynamics) may undergo changes with increasing age of the person. If appropriate it is important to specify a recommended usage period of biometric reference data.

7.4 Enrolment conditions

In order to achieve good comparison results, it is important to specify enrolment conditions with respect to the minimum quality of the biometric reference data, e.g. minimum number of minutiae or, in the case of image data, minimum focus quality, contrast, spatial sampling rate, etc.

7.5 Feature extraction algorithms

If biometric data formats for interchange are specified at the feature level (e.g. finger minutiae), then the way for deriving these features shall be specified to the extent necessary to facilitate interoperability, i.e. the comparison results of different implementations shall be within the range of allowed differences.

7.6 Feature comparison algorithms

If biometric data formats for interchange are specified at the feature level (e.g. finger minutiae), then the means for comparing the biometric probe against the biometric references generated in an enrolment process shall be specified to the extent necessary to facilitate interoperability, i.e. the comparison results of different implementations shall be within the range of allowed differences.

8 Processing level of data formats for interchange

8.1 Processing levels according to ISO/IEC 19785-1

The processing levels of biometric data as defined in ISO/IEC 19785-1:2006 are the following:

— captured biometric sample: the data in its raw form as delivered by the capture device,

— intermediate data: the data has been processed from the form delivered by the sensor, but is not in a form usable for comparison – these data are addressed as image data or behavioural data,

— processed data: the data is in a form that can be used for comparison - these data are addressed as feature data.

For interchange, intermediate data (image or behavioural data) and feature data as shown in Figure 3 are of special relevance.

Examples of scenarios using biometric data of different processing level are shown in Annex A.

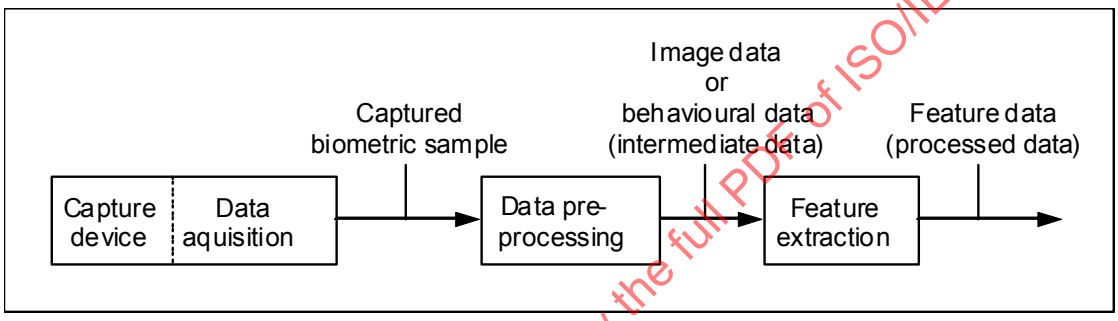

Figure 3 — Sensor data, image/behavioural data and feature data

8.2 Captured biometric sample

The captured biometric sample is influenced by some or all of the following:

— underlying biometric characteristic that is the bodily source,

— presentation of the biometric characteristic to the capture device,

— data pre-processing (as part of data acquisition) within the capture device,

— performance of the sensor and capture device,

— environmental conditions (e.g. lighting, background noise),

Captured biometric samples are usually not used for interchange.

8.3 Image data

In many cases, the acquired biometric data of a static biometric characteristic delivered by a biometric capture device is subsampled, scaled, interpolated, compressed or otherwise processed to produce an image of the characteristic. The first important convention to be made concerns the general image file format (e.g. BMP, TIFF, GIF, JPEG, JPEG-LS, JPEG2000) and the compression level to make images readable for all systems. Further conventions are needed for certain parameters concerning the image capturing process and the hardware to be used which have a strong impact on the resulting image e.g. bit depth (e.g. 8 bit, 16 bit), spatial sampling rate, position of biometric characteristic to be represented, and lighting conditions during image capture process.

8.4 Behavioural data

In contrast to the acquisition of image data, which captures a static anatomical characteristic like a fingerprint, a behavioural biometric characteristic is a dynamic action with contributions from conditioned behaviour patterns as well as anatomical characteristics. For behavioural biometric characteristics, common acquisition methods are provided by time-based and frequency-based analysis. Therefore, the standardization has concentrated on data formats for these approaches.

8.5 Feature data

Feature data may consist of several feature data units. A feature data unit may consist of several data elements, e.g. coordinates and angles. The structure and content of a feature data unit depends on the biometric modality.

8.6 Naming conventions for biometric data formats

The name of the data structure should indicate the biometric modality and, where different feature data structures are available, the respective feature. For example,

— finger minutiae data,

— finger image data,

— signature/sign time series data,

— hand geometry silhouette data,

— voice data,

— DNA data.

8.7 Recommendations for standardizing biometric data formats

The standardization of biometric data formats is intended to provide interoperability. Thus the number of standardized formats should be kept small and manageable. The following qualifications should be considered before a new data format may enter a standardization process:

— the data format represents the essential data required for an alternative mathematical approach of feature extraction and/or comparison,

— the data format is a prevalent alternative representation of data that is not defined in ISO/IEC 19794,

— the data format represents data of a widely-used biometric modality not considered in ISO/IEC 19794 yet,

— the data format represents data of a different processing level and has become widely-used for data interchange or has the potential for it,

— the data format enables interoperability among algorithms that use individual non-standardized data formats of a more advanced processing level,

— the data format drastically reduces the size of data of an already standardized data format and is suitable for usage on card/token,

— the data format has the potential to be used for different biometric modalites, e.g. an image format,

— the data format combines existing formats without increasing size,

— the data format allows increase in biometric performance.

9 Multibiometrics

Multibiometrics can be divided in five sub-categories, which are defined in ISO/IEC TR 24722:

— multimodal – usage of different biometric modalities such as face and fingerprint,

— multialgorithmic – usage of two or more distinct algorithms for processing the same biometric sample,

— multiinstance – usage of at least two instances of the same biometric modality e.g. left and right iris or left and right pointer finger,

— multisensorial – using multiple capture devices for capturing samples of one biometric instance,

— 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.

Multibiometrics may be used to improve the performance of biometric systems in terms of error rates. If multimodal biometric systems are used, data structures of several parts of ISO/IEC 19794 may be involved in a verification or identification process. Multi-instance or multi-presentation data are stored in several biometric representations that are contained in one record.

10 Capture device requirements

Capture device requirements should be defined to such an extent as it is necessary to achieve interoperability. Subject of these definitions may include:

— capture device technology,

— spatial sampling rate,

— size,

— range of grey or colour level,

— sample rate,

— illumination type and intensity,

— signal to noise ratio.

The capture device technology identifier shall indicate the class of capture device technology that was used to acquire the captured biometric sample (e.g. optical or capacitive fingerprint sensor). The capture device vendor identifier and the capture device type identifier represent an IBIA registered vendor and a specific device model of that vendor. The certification block represents the certification schemes that were applied in the quality evaluation of the capture device.

11 Format owner and format types

11.1 Relationship to CBEFF

ISO/IEC 19785 (Common Biometric Exchange Formats Framework – CBEFF) provides generic containers for biometric data. ISO/IEC 19785-1 specifies the general CBEFF concepts and a number of abstract data elements. ISO/IEC 19785-2 contains provisions for the operation of a CBEFF registration authority, responsible for the allocation of distinctive identifiers for organisations, formats, and products and for the maintenance of an official registry. ISO/IEC 19785-3 defines, using abstract CBEFF data elements defined in

ISO/IEC 19785-1 and possibly additional data elements, a number of CBEFF patron formats for particular domains of use.

CBEFF defines a common set of data elements to support multiple technologies. It describes a biometric information record (BIR) consisting of a standard biometric header (SBH), a biometric data block (BDB) and a security block (SB) as Figure 4 shows. The BDB is the structural unit for the insertion of biometric data interchange formats as defined in ISO/IEC 19794.

An ISO/IEC 19794 conformant record may be embedded in a CBEFF wrapper. In that situation the record is referred to as a BDB. A record without a CBEFF wrapper is referred to as a biometric data interchange record (BDIR). The CBEFF wrapper is not required for conformance to ISO/IEC 19794.

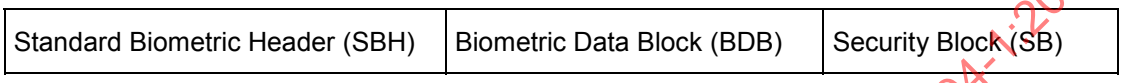

Figure 4 — CBEFF biometric information record (source: ISO/IEC 19785-1)

CBEFF supports patron formats to meet specific application environments. When using smart cards, data structures as defined in ISO/IEC 7816-11 and in the smart card related clauses of ISO/IEC 19785-3 shall be used.

A CBEFF patron format is a full, bit-level specification of encodings containing one or more biometric data blocks (BDB's) together with information identifying the BDB formats and possibly further information. A data structure encoded in accordance with a CBEFF patron format is referred to as a BIR. The header part of a CBEFF-compliant BIR includes for each BDB the CBEFF data element BDB format owner, serving to identify the organisation that has defined the format of the BDB, and the CBEFF data element BDB format type, serving to identify that format within the scope of the format owner.

NOTE A BDIR need not be embedded in a CBEFF-compliant BIR if it is known from the context which format was used for encoding it.

11.2 BDB format owner

The BDB format owner of all biometric data interchange formats defined in ISO/IEC 19794 is ISO/IEC JTC 1/SC 37. The BDB format owner identifier for ISO/IEC JTC 1/SC 37 as registered by the CBEFF registration authority IBIA is 257 (0101_{Hex}).

The other registered format owners are listed in www.ibia.org.

11.3 BDB format types

Each biometric data interchange format defined in ISO/IEC 19794 is identified by a BDB format type identifier to be used in situations when the BDIR is embedded in a CBEFF wrapper. Each BDB format type identifier is coded in 2 bytes. The value is assigned by ISO/IEC JTC 1/SC 37 and registered with the CBEFF registration authority IBIA.

NOTE The same part of ISO/IEC 19794 can define more than one biometric data interchange format type.

In each part of ISO/IEC 19794, for each biometric data interchange format defined in that part, the BDB format type identifier, the BDB format type short name, and the BDB format type full object identifier registered with the CBEFF registration authority IBIA shall be listed.

All registered BDB format type information is also listed in www.ibia.org.

12 Coding scheme for format types

12.1 Structure of data records

Each of ISO/IEC 19794-2 through ISO/IEC 19794-*n* includes clauses defining data interchange formats – at least one full or record format for general use and possibly several compact formats for use with smart cards and other tokens. Furthermore, each part shall have an Annex that specifies elements of conformance testing methodology, test assertions, and test procedures as applicable to that specific part.

Some compact formats only represent data from a single biometric sample, while all full or record formats are capable of recording data from multiple samples, each one contained in a separate "representation" record. Formats accommodating multiple representations generally have the structure shown in Figure 5, where the BDIR is comprised of a general record header (storing metadata applicable to all representations) and one or more representation records. Each representation record contains a header (storing representation-specific metadata) and biometric data. Unless otherwise specified, all values are fixed-length unsigned integer or unsigned short quantities represented in Big-Endian format where the more significant bytes of any multi-byte quantity are stored at lower memory addresses than (and are transmitted before) less significant bytes.

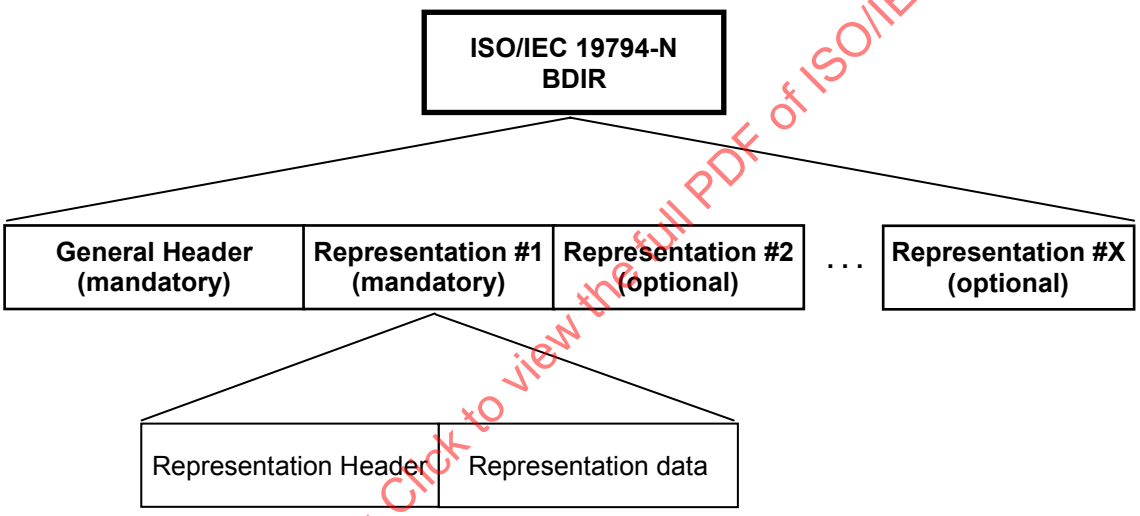

Figure 5 — Example structure of a multiple-representation BDIR

12.2 Common elements for the general header

The General Header is defined separately for each part of ISO/IEC 19794, though some commonality does exist. The General Header of each record format defined in the other parts of ISO/IEC 19794 shall contain the fields listed in Table 1. These fields shall be in the given order and shall be the first ones in the General Header. Their definition should follow the harmonized text in Table 1.

Table 1 — Mandatory elements of the general header

Name	Length	Harmonized text
Format identifier	4 bytes	The format identifier shall be recorded in four bytes. The format identifier shall consist of three characters "xxx" followed by a zero byte as a NULL string terminator. NOTE The ASCII characters “xxx” for the record formats defined in each part of ISO/IEC 19794 are defined in Table 2.
Version number	4 bytes	The number for the version of that part of ISO/IEC 19794 used for constructing the BDIR shall be placed in four bytes. This version number shall consist of three ASCII numerals followed by a zero byte as a NULL string terminator. The first and second character will represent the major version number and the third character will represent the minor revision number. EXAMPLE Upon approval of a specification, the initial version number will be “010” – Version 1 revision 0. NOTE The correct version and revision number of the actual part should be used.
Length of record	4 bytes	The length (in bytes) of the entire BDIR shall be recorded in four bytes. This count shall be the total length of the BDIR including the general record header and one or more representation records.
Number of representations	2 bytes	The total number of representation records contained in the BDIR shall be recorded in two bytes. A minimum of one representation is required.
Certification flag	1 byte	For record formats that allow certification blocks: The one-byte certification flag shall indicate whether each Representation Header includes a certification block. A value of 00_{Hex} shall indicate that no representation contains a certification block. A value of 01_{Hex} shall indicate that all representations contain a certification block. NOTE A certification block that is present may contain 0 certifications (in that case the number-of-certifications field in the certification block has the value 0). For record formats that have no certification blocks defined: The one-byte certification flag indicates whether each representation header includes a certification block. Its value shall be 00_{Hex} to indicate that no representation contains a certification block. NOTE The certification flag has been added for upward compatibility with later versions of the record format in which representation headers may contain certification blocks.

Table 2 — Format identifiers

ISO/IEC 19794 part number	2	3	4	5	6	7	8	9	10	11	13	14
Format identifier	“FMR”	"FSP"	"FIR"	“FAC”	“IIR”	“SDI”	“FSK”	"VIR"	“HND”	“SPD”	“VDI”	“DNA”

12.3 Common elements for the representation headers

12.3.1 Overview

The Representation Header is defined separately for each record format of ISO/IEC 19794, though some commonality does exist. The Representation Header of each record format defined in the other parts of ISO/IEC 19794 shall contain the fields listed in Table 3. These fields shall be in the given order and shall be the first ones in the Representation Header. Their definition should follow the harmonized text in Table 3.

Table 3 — Mandatory elements of the representation header

Name	Length	Harmonized text for record format definitions
Representation length	4 bytes	The representation-length field denotes the length in bytes of the representation including the representation header fields.
Capture date and time	9 bytes	The capture date and time field shall indicate when the capture of this representation started in Coordinated Universal Time (UTC). The capture date and time field shall consist of 9 bytes. Its value shall be encoded in the form given in ISO/IEC 19794-1.
Capture device technology identifier	1 byte	The capture device technology ID shall be encoded in one byte. This field shall indicate the class of capture device technology used to acquire the captured biometric sample. A value of 00_{Hex} indicates unknown or unspecified technology. See Table N for the list of possible values. NOTE N is to be replaced with the correct table number in the corresponding part of ISO/IEC 19794.

After the mandatory elements specified in Table 3, other fields may be defined for the Representation Header of a particular record format defined in ISO/IEC 19794. The first of those fields, if applicable, shall be the ones defined in Table 4, with the order as shown. The format definition shall follow the harmonized text shown in Table 4.

Table 4 — Optional elements of the representation header

Name	Length	Harmonized text for record format definitions
Capture device vendor identifier	2 bytes	The capture device vendor identifier shall identify the biometric organisation that owns the product that created the BDIR. The capture device algorithm vendor identifier shall be encoded in two bytes carrying a CBEFF biometric organization identifier (registered by IBIA or other approved registration authority). A value of all zeros shall indicate that the capture device vendor is unreported.
Capture device type identifier	2 bytes	The capture device type identifier shall identify the product type that created the BDIR. It shall be assigned by the registered product owner or other approved registration authority. A value of all zeros shall indicate that the capture device type is unreported. If the capture device vendor identifier is 0000_{Hex}, then also the capture device type identifier shall be 0000_{Hex}.
Quality record	1 to 1,276 bytes (1 to 1 + (255 * 5))	A quality record shall consist of a length field followed by zero or more quality sub-blocks. The length field shall consist of one byte. It shall represent the number of quality blocks as an unsigned integer. Each quality block shall consist of – a quality score, – a quality algorithm vendor identifier, and – a quality algorithm identifier. A quality score should express the predicted comparison performance of a representation. A quality score shall be encoded in one byte as an unsigned integer. Allowed values are – 0 to 100 with higher values indicating better quality, – 255, i.e. ff_{Hex}, for indicating that an attempt to calculate a quality score failed. The quality algorithm vendor identifier shall identify the provider of the quality algorithm. The quality algorithm vendor identifier shall be encoded in two bytes carrying a CBEFF biometric organization identifier (registered by IBIA or other approved registration authority). A value of all zeros shall indicate that the value for this field is unreported.

		The quality algorithm identifier shall identify the vendor's quality algorithm that created the quality score. It shall be assigned by the provider of the quality algorithm or an approved registration authority. The quality algorithm identifier shall be encoded in two bytes. A value of all zeros shall indicate that the value for this field is unreported.
Certification record	1 to 766 bytes (1 to 1 + (255 * 3))	The certification record only exists if the certification flag in the general header has a value of 1. A certification record shall consist of a length field followed by zero or more certification blocks. The length field shall consist of one byte. It shall represent the number of unique certification blocks as an unsigned integer. Each certification block shall consist of – a certification authority identifier and – a certification scheme identifier. The certification authority identifier shall identify a certification authority that has carried out a certification according to a certification scheme. The certification authority identifier shall be encoded in two bytes carrying a CBEFF biometric organization identifier (registered by IBIA or other approved registration authority). The certification scheme identifier shall identify a certification scheme according to which a certification has been carried out. The certification scheme identifier shall be encoded in one byte. See Table M for the list of certification scheme identifiers. NOTE M is to be replaced with the correct table number in the corresponding part of ISO/IEC 19794.

12.3.2 Common format for date and time

Date and time within a representation header shall be stated in Coordinated Universal Time (UTC). This format shall be used for any absolute time values in representation headers. The representation headers shall include the capture date and time. The encoding date and time are optional.

A date and time field shall consist of

— a two-byte field representing the ordinal number of a calendar year (1 to 65534) as an unsigned integer,

— a one-byte field representing the ordinal number of a calendar month within the calendar year (1 to 12) as an unsigned integer,

— a one-byte representing the ordinal number of a calendar day within the calendar month (1 to 31) as an unsigned integer,

— a one-byte field representing the ordinal number of an hour on the given date (0 to 23) as an unsigned integer,

— a one-byte field representing the ordinal number of a minute within the hour (0 to 59) as an unsigned integer,

— a one-byte field representing the ordinal number of a second within the minute (0 to 59) as an unsigned integer, and

— a two-byte field representing the ordinal number of a millisecond within the second (0 to 999) as an unsigned integer.

If a one-byte component of date and time is unknown, then it shall have the value ff_{Hex}. If a two-byte component of date and time is unknown, then it shall have the value $ffff_{Hex}$. If a component of date and time is unknown, then also all subsequent components shall be unknown.

EXAMPLE Thursday 17:35:20 December 15, 2005 is encoded as 07 d50c 0f11 2314 $ffff_{Hex}$.