INTERNATIONAL STANDARD

ISO/IEC 2382-37

Second edition
2017-02

Information technology — Vocabulary —

Part 37: Biometrics

Technologies de l'information — Vocabulaire — Partie 37: Biométrie

Reference number
ISO/IEC 2382-37:2017(E)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

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 and 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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, Subcommittee SC 37, *Biometrics*.

This second edition cancels and replaces the first edition (ISO/IEC 2382-37:2012). Minor changes have been made to some of the terms published in the 2012 edition and 41 new terms have been added.

Introduction

The main purpose of this document is to provide a systematic description of the concepts in the subject field of biometrics and to clarify the use of the terms in this subject field. The subject field of biometrics is broken down into subfields.

This document is addressed to biometrics standardizers and to users of these standards.

Terms defined in this document are to be understood in the subject field of biometrics. When terms exist in various subject fields, the current subject field may be indicated in angle brackets.

Words that are **bolded** are defined in this document. Words that are not **bolded** are to be understood in their natural language sense. The authority for natural language use of terms in this document is the Concise Oxford English Dictionary, Thumb Index Edition (tenth edition, revised, 2002).

EXAMPLE

candidate

<biometrics> *biometric reference identifier* (3.3.19) of a *biometric reference* (3.3.16) in the *biometric reference database* (3.3.17) determined to be similar to the *biometric probe* (3.3.14)

candidate

<politics> a person who applies for a job or is nominated for election

NOTE When using terms defined with a qualifier (for example, “biometric xxx”), it is normal to include the qualifier on the first occurrence of the term in every paragraph, but to omit it on subsequent occurrences of that term within the same paragraph. In broader contexts, where the qualifier (in this case, ‘biometric’) is clearly understood, then the qualifier may be omitted completely.

The terms in this document are listed in a systematic order under a number of general headings.

The layout follows the directions given in ISO 10241-1. Thus, the elements of an entry appear in the following order:

— Entry number (mandatory);

— Preferred term(s) (mandatory);

— Admitted term(s) (mandatory);

— Deprecated term(s);

— Definition;

— Example(s);

— Note(s).

Information technology — Vocabulary —

Part 37:
Biometrics

1 Scope

This document establishes a systematic description of the concepts in the field of biometrics pertaining to recognition of human beings and reconciles variant terms in use in pre-existing biometric standards against the preferred terms, thereby clarifying the use of terms in this field.

Excluded from the scope of this document are concepts (represented by terms) from information technology, pattern recognition, biology, mathematics, etc. Biometrics uses such fields of knowledge as a basis.

In principle, mode specific terms are outside of scope of this document.

Words that are **bolded** are defined in this document. Words that are not bolded are understood in their natural language sense. The authority for natural language use of terms in this document is the Concise Oxford English Dictionary, Thumb Index Edition (tenth edition, revised, 2002). Words used in their natural language sense are considered out-of-scope for further definition in this document.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

3.1 General concept terms

3.1.1
biometric (adjective)
of or having to do with *biometrics* (3.1.3)

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 mode* (3.2.5) most suited to the practicalities of travel documents.

EXAMPLE 3 Incorrect usage #2: The **biometric** recorded in my passport is a facial image.

EXAMPLE 4 Correct usage #2: The *biometric characteristic* (3.1.2) recorded in my passport is a facial image.

Note 1 to entry: The use of **biometric** as a noun, to mean for example, *biometric characteristic* (3.1.2), is deprecated.

Note 2 to entry: Since the late 19th century, the designations 'biometrics' and 'biometry' have been used with the general meaning of counting, measuring and statistical analysis of any kind of data in the biological sciences including the relevant medical sciences.

3.1.2
biometric characteristic
DEPRECATED: biometric (noun)
biological and behavioural characteristic of an individual from which distinguishing, repeatable *biometric features* (3.3.11) can be extracted for the purpose of *biometric recognition* (3.1.3)

EXAMPLE Examples of **biometric characteristics** are: Galton ridge structure, face topography, facial skin texture, hand topography, finger topography, iris structure, vein structure of the hand, ridge structure of the palm, retinal pattern, handwritten signature dynamics, etc.

3.1.3
biometric recognition
biometrics
automated recognition of individuals based on their biological and behavioural characteristics

Note 1 to entry: In the field of **biometrics** (as defined in this document), "Individual" is restricted in scope to refer only to humans.

Note 2 to entry: The general meaning of **biometrics** encompasses counting, measuring and statistical analysis of any kind of data in the biological sciences including the relevant medical sciences.

Note 3 to entry: **Biometric recognition** encompasses *biometric verification* (3.8.3) and *biometric identification* (3.8.2).

Note 4 to entry: Automated recognition implies that a machine based system is used for the recognition either for the full process or assisted by a human being.

Note 5 to entry: Behavioural and biological characteristics cannot be completely separated which is why the definition uses 'and' instead of 'and/or'. For example, a fingerprint image results from the biological characteristics of the finger ridge patterns and the behavioural act of presenting the finger.

Note 6 to entry: Use of 'authentication' as a synonym for "*biometric verification* (3.8.3) or *biometric identification* (3.8.2)" is deprecated; the term **biometric recognition** is preferred.

3.2 Biometric system terms

3.2.1
biometric capture subsystem
biometric capture devices (3.4.1) and any sub-processes required to execute a *biometric capture process* (3.5.2)

Note 1 to entry: In some systems, converting a signal from a *biometric characteristic* (3.1.2) to a *captured biometric sample* (3.3.25) may include multiple components such as a camera, photographic paper, printer, digital scanner, ink and paper.

Note 2 to entry: A **biometric capture subsystem** can consist of only a single *biometric capture device* (3.4.1).

3.2.2
biometric identification system
system that aims to perform *biometric identification* (3.8.2)

3.2.3
biometric system
system for the purpose of the *biometric recognition* (3.1.3) of individuals based on their behavioural and biological characteristics

Note 1 to entry: A **biometric system** will contain both *biometric* (3.1.1) and non-biometric components.

3.2.4
biometric verification system
system that aims to perform *biometric verification* (3.8.3)

3.2.5
mode
DEPRECATED: biometric (noun)
combination of a *biometric characteristic* (3.1.2) type, a sensor type and a processing method

Note 1 to entry: The processing algorithm may contain multiple methods, details of which may not be externally apparent. Thus a *biometric system* (3.2.3) is considered as using one processing method, until it is otherwise specified.

Note 2 to entry: Determining what constitutes a single type of sensor, processing method or *biometric characteristic* (3.1.2) will depend on convention. For example, current convention is that images of ridge patterns from both thumbs and fingers represent a single *biometric characteristic* (3.1.2) type, i.e. fingerprints. With respect to sensors, infrared and optical bandwidth sensors are considered different types, but optical bandwidth sensors are considered a single type despite imaging red, green and blue bandwidths.

3.2.6
multi-modal
multiple in at least 2 out of 3 constituents of a *mode* (3.2.5) in a single *biometric system* (3.2.3)

Note 1 to entry: Multiple implies difference in type.

3.2.7
system participation ratio
proportion of individuals eligible to use the system who do use the system

Note 1 to entry: Enrolled individuals are a subset of eligible individuals.

3.3 Terms for data in biometric systems

3.3.1
anonymized biometric data record
biometric data record (3.3.8) purposely disassociated from individual metadata

Note 1 to entry: The *biometric data* (3.3.6) within the *biometric data record* (3.3.8) ultimately remains attributable to an individual.

3.3.2
biometric application database
database of *biometric data* (3.3.6) and associated metadata developed from and supporting the operation of a *biometric* (3.1.1) application

Note 1 to entry: The metadata may include transaction history; authorizations (e.g. age) of *biometric data subject* (3.7.5); and archived *biometric data* (3.3.6).

Note 2 to entry: The term application includes the policies that govern the operation of the system and evidence of that operation.

3.3.3
biometric application decision
decision to perform an action at the application level based on the results of a *biometric* (3.1.1) process

Note 1 to entry: The application decision may include more than a *comparison* (3.5.7) process. For example, a *biometric capture process* (3.5.2) may show that there are no characteristics to capture and a decision can be made on this before any *biometric characteristics* (3.1.2) are compared.

Note 2 to entry: **Biometric application decisions** can be made on the basis of complex policies involving both *biometric* (3.1.3) and non-biometric data.

3.3.4
biometric candidate
biometric reference identifier (3.3.19) of a *biometric reference* (3.3.16) in the *biometric reference database* (3.3.17) determined to be sufficiently similar to the *biometric probe* (3.3.14) to warrant further analysis

3.3.5
biometric candidate list
set of zero, one or more *biometric candidates* (3.3.4) that may be intermediate or final

Note 1 to entry: Intermediate **biometric candidate lists** may be produced by systems that use multi-pass *biometric identification* (3.8.2).

Note 2 to entry: **Biometric candidate lists** may or may not be ordered.

3.3.6
biometric data
biometric sample (3.3.21) or aggregation of *biometric samples* (3.3.21) at any stage of processing, e.g. *biometric reference* (3.3.16), *biometric probe* (3.3.14), *biometric feature* (3.3.11) or *biometric property* (3.3.15)

Note 1 to entry: **Biometric data** need not be attributable to a specific individual, e.g. Universal Background Models.

3.3.7
biometric database
database of *biometric data record(s)* (3.3.8)

3.3.8
biometric data record
data record containing *biometric data* (3.3.6)

Note 1 to entry: A **biometric data record** may include non-biometric data.

3.3.9
biometric enrolment database
database of *biometric enrolment data record(s)* (3.3.10)

Note 1 to entry: A database of *biometric data* (3.3.6) not attributable to *biometric data subjects* (3.7.5) is a *biometric database* (3.3.7), but not a **biometric enrolment database**, e.g. a database utilised in the training of a Universal Background Model.

Note 2 to entry: The **biometric enrolment database** may or may not contain the *biometric reference database* (3.3.17). Separation of the databases may be required due to security, privacy, legislation, architecture, performance, etc.

Note 3 to entry: A single *biometric reference* (3.3.16) (e.g. a fingerprint on a storage card) may be considered as a **biometric enrolment database** in some transactions.

3.3.10
biometric enrolment data record
data record attributed to a *biometric data subject* (3.7.5), containing non-biometric data and associated with *biometric reference identifier(s)* (3.3.19)

Note 1 to entry: Data can be updated after enrolment.

Note 2 to entry: The **biometric enrolment data record** will either contain *biometric reference data record(s)* (3.3.18) or pointer(s) to *biometric reference data record(s)* (3.3.18).

Note 3 to entry: The associated *biometric reference* (3.3.16) may be null (for example, *biometric enrolee* (3.7.6) lacks the *biometric characteristic* (3.1.2) or a *biometric capture process* (3.5.2) is pending).

3.3.11
biometric feature
numbers or labels extracted from *biometric samples* (3.3.21) and used for *comparison* (3.5.7)

Note 1 to entry: **Biometric features** are the output of a completed *biometric feature extraction* (3.5.4).

Note 2 to entry: The use of this term should be consistent with its use by the pattern recognition and mathematics communities.

Note 3 to entry: A **biometric feature** set can also be considered a processed *biometric sample* (3.3.21).

Note 4 to entry: **Biometric features** may be extracted from an *intermediate biometric sample* (3.3.30).

Note 5 to entry: Filters applied to *biometric samples* (3.3.21) are not themselves **biometric features**, however the output of the filter applied to these samples may be. Therefore, for example, eigenfaces are not **biometric features.**

3.3.12
biometric identification decision
comparison decision (3.3.26) as to whether a *biometric reference(s)* (3.3.16) of a particular *biometric data subject* (3.7.5) is in a *biometric reference database* (3.3.17)

Note 1 to entry: Return of a *biometric candidate list* (3.3.5) is not considered a **biometric identification decision**.

Note 2 to entry: A positive *biometric identification* (3.8.2) process is inferred from the output of a *biometric reference identifier* (3.3.19).

3.3.13
biometric model
stored function generated from *biometric data (3.3.6)*

EXAMPLE Examples of **biometric models** could be a Hidden Markov Model, Gaussian Mixture Model or an Artificial Neural Network.

Note 1 to entry: In most occasions, the **biometric model** is a stored function which is dependent on the *biometric data subject (3.7.5)*.

Note 2 to entry: The function may be determined through training.

Note 3 to entry: A **biometric model** may involve intermediate processing similar to *biometric feature extraction* (3.5.4).

3.3.14
biometric probe
biometric query
biometric sample (3.3.21) or *biometric feature* (3.3.11) set input to an algorithm for *biometric comparison* (3.5.7) to a *biometric reference(s)* (3.3.16)

Note 1 to entry: In some *comparisons* (3.5.7), a *biometric reference* (3.3.16) might be used as the subject of the comparison with other *biometric references* (3.3.16) or incoming *biometric samples* (3.3.21) used as the objects of the *comparisons* (3.5.7). For example, in a duplicate enrolment check, a *biometric reference* (3.3.16) will be used as the subject for *comparisons* (3.5.7) against all *other biometric references* (3.3.16) in the database.

Note 2 to entry: Typically in a biometric *comparison* (3.5.7) process, incoming *biometric samples* (3.3.21) serve as the subject of *comparisons* (3.5.7) against objects stored as *biometric references* (3.3.16) in a database.

3.3.15
biometric property
descriptive attributes of the *biometric data subject* (3.7.5) estimated or derived from the *biometric sample* (3.3.21) by automated means

EXAMPLE Fingerprints can be classified by the **biometric properties** of ridge-flow, i.e. arch, whorl, and loop types. Estimates of age or gender from face recognition would also be **biometric properties**.

3.3.16
biometric reference
one or more stored *biometric samples* (3.3.21), *biometric templates* (3.3.22) or *biometric models* (3.3.13) attributed to a *biometric data subject* (3.7.5) and used as the object of *biometric comparison* (3.5.7)

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

Note 1 to entry: A **biometric reference** may be created with implicit or explicit use of auxiliary data, such as Universal Background Models.

Note 2 to entry: The subject/object labelling in a *comparison* (3.5.7) might be arbitrary. In some *comparisons* (3.5.7), a **biometric reference** might be used as the subject of the comparison with other **biometric references** or incoming samples and input to an algorithm for biometric comparison (3.5.7). For example, in a duplicate enrolment check a **biometric reference** will be used as the subject for comparison against all other **biometric references** in the database.

3.3.17
biometric reference database
database of *biometric reference data records* (3.3.18)

Note 1 to entry: The **biometric reference database** may be a subset of the *biometric enrolment database* (3.3.9), or it may be a separate database. Separation of the databases may be required due to security, privacy, legislation, architecture, performance, etc.

3.3.18
biometric reference data record
indexed data record containing *biometric reference(s)* (3.3.16)

Note 1 to entry: There may not be a one-to-one correspondence between **biometric reference data records** and *biometric data subjects* (3.7.5), e.g. a single *biometric data subject* (3.7.5) might have several reference data records and in some applications, a single **biometric reference data record** might be associated with multiple enrolments of a *biometric data subject* (3.7.5).

3.3.19
biometric reference identifier
pointer to a *biometric reference data record* (3.3.18) in the *biometric reference database* (3.3.17)

3.3.20
biometric representation
biometric sample (3.3.21) or *biometric feature* (3.3.11) set

Note 1 to entry: This term is used in ISO/IEC 19794 biometric data interchange format standards for labelling a sub-record in a *biometric data record* (3.3.8).

3.3.21
biometric sample
analog or digital representation of *biometric characteristics* (3.1.2) prior to *biometric feature extraction* (3.5.4)

EXAMPLE A record containing the image of a finger is a **biometric sample.**

3.3.22
biometric template
reference biometric feature set
set of stored *biometric features* (3.3.11) comparable directly to probe *biometric features* (3.3.11)

EXAMPLE A record containing a set of finger minutiae is a **biometric template.**

Note 1 to entry: A *biometric reference* (3.3.16) consisting of an image, or other *captured biometric sample* (3.3.25), in its original, enhanced or compressed form, is not a **biometric template**.

Note 2 to entry: The *biometric features* (3.3.11) are not considered to be a **biometric template** unless they are stored for reference.

3.3.23
biometric verification decision
comparison decision (3.3.26) determining the validity of a *biometric claim* (3.6.4) in a *verification transaction* (3.6.21)

3.3.24
biometric candidate score
comparison score (3.3.27) for a *biometric candidate* (3.3.4)

3.3.25
captured biometric sample
DEPRECATED: raw biometric sample
biometric sample (3.3.21) resulting from a *biometric capture process* (3.5.2)

3.3.26
comparison decision
determination of whether the *biometric probe(s)* (3.3.14) and *biometric reference(s)* (3.3.16) have the same *biometric* (3.1.1) source, based on a *comparison score(s)* (3.3.27), a decision policy(ies) including a *threshold* (3.3.36), and possibly other inputs

Note 1 to entry: A *match* (3.3.31) is a positive **comparison decision**. A *non-match* (3.3.33) is a negative **comparison decision**. A decision of "undetermined" may sometimes be given.

3.3.27
comparison score
DEPRECATED: matching score
numerical value (or set of values) resulting from a *comparison* (3.5.7)

Note 1 to entry: Higher does not necessarily mean more similar.

3.3.28
dissimilarity score
distance score
comparison score (3.3.27) that decreases with similarity

Note 1 to entry: Unlike a **distance score,** a **dissimilarity score** does not have to meet the mathematical definition of a metric on a set.

3.3.29
fraudulent biometric enrolment data record
biometric enrolment data record (3.3.10) created or modified for the purpose of supporting wrongful or criminal activity

Note 1 to entry: Records that are inadvertently erroneous or created for test purposes are not considered fraudulent.

3.3.30
intermediate biometric sample
biometric sample (3.3.21) resulting from *intermediate biometric sample processing* (3.5.9)

EXAMPLE *Biometric samples* (3.3.21) that have been cropped, down-sampled, compressed, or enhanced are examples of **intermediate biometric samples.**

3.3.31
match (noun)
comparison decision (3.3.26) stating that the *biometric probe(s)* (3.3.14) and the *biometric reference* (3.3.16) are from the same source

Note 1 to entry: Historically, the word **match** has been used as a verb to indicate the act of comparison and decision making. As 'match' is the decision coming out of the *comparison* (3.5.7) process, its use as a verb is deprecated in favour of compare.

3.3.32
mated (adjective)
of or having to do with a paired *biometric probe* (3.3.14) and *biometric reference* (3.3.16) that are from the same *biometric characteristic* (3.1.2) of the same *biometric data subject* (3.7.5)

Note 1 to entry: While '*match* (3.3.31)' is the result of a biometric *comparison decision* (3.3.26), '**mated**' is a statement, based on non-biometric information, concerning the origin of the source of the *biometric probe* (3.3.14) and the *biometric reference* (3.3.16).

3.3.33
non-match (noun)
comparison decision (3.3.26) stating that the *biometric probe(s)* (3.3.14) and the *biometric reference* (3.3.16) are not from the same source

3.3.34
non-mated (adjective)
of or having to do with a paired *biometric probe* (3.3.14) and *biometric reference* (3.3.16) that are not from the same *biometric characteristic* (3.1.2) of the same *biometric data subject* (3.7.5)

Note 1 to entry: While '*non-match* (3.3.33)' is the result of a biometric *comparison decision* (3.3.26), '**non-mated**' is a statement, based on non-biometric information, concerning the origin of the source of the *biometric probe* (3.3.14) and the *biometric reference* (3.3.16).

3.3.35
similarity score
comparison score (3.3.27) that increases with similarity

3.3.36
threshold (noun)
numerical value (or set of values) at which a decision boundary exists

3.3.37
unidentified biometric data
biometric data (3.3.6) whose *biometric data subject* (3.7.5) is currently unknown

3.3.38
conformant biometric reference rate
proportion of *biometric enrolment data records* (3.3.10) containing *biometric references* (3.3.16) conformant with system policy

Note 1 to entry: Some *biometric systems* (3.2.3) require the enrolment of all applicants regardless of the availability of acquirable *biometric characteristics* (3.1.2). This ratio, which depends upon system capabilities and policies regulating acquisition of *biometric samples* (3.3.21), characterizes the percentage of a given enrolled population that has conformant *biometric references* (3.3.16) in the biometric *enrolment data records* (3.3.10).

Note 2 to entry: This can be enumerated individually for enrolment subsystems with distinct enrolment policies.

3.3.39
biometric reference rate
proportion of *biometric enrolment data records* (3.3.10) that contain a *biometric reference* (3.3.16)

Note 1 to entry: Some *biometric systems* (3.2.3) require the enrolment of all applicants regardless of the availability of acquirable *biometric characteristics* (3.1.2). This ratio, which depends upon system capabilities and policies regulating acquisition of *biometric samples* (3.3.21), characterizes the percentage of a given enrolled population that has any *biometric references* (3.3.16) in the *biometric enrolment data records* (3.3.10).

Note 2 to entry: This can be enumerated individually for enrolment subsystems with distinct enrolment policies.

Note 3 to entry: Non-conformant references are considered as references.

3.3.40
enrolment eligibility ratio
proportion of enrolment applications that are deemed eligible by policy for enrolment

Note 1 to entry: The closer this ratio is to unity the more aligned the applicants are to the eligible population.

3.3.41
reference ageing
changes in error rates with respect to a fixed reference caused by time-related changes in the *biometric characteristic* (3.1.2)

Note 1 to entry: Error rates generally increase with the age of the reference.

3.4 Device terms

3.4.1
biometric capture device
device that collects a signal from a *biometric characteristic* (3.1.2) and converts it to a *captured biometric sample* (3.3.25)

Note 1 to entry: A signal can be generated by the *biometric characteristic* (3.1.2) or generated elsewhere and affected by the *biometric characteristic* (3.1.2), for example, face illuminated by incident light.

Note 2 to entry: A **biometric capture device** can be any piece of hardware (and supporting software and firmware).

Note 3 to entry: A **biometric capture device** may comprise components such as an illumination source, one or more biometric sensors, etc.

3.5 Functioning terms

3.5.1
biometric acquisition process
biometric capture process (3.5.2) and additional processing to attempt to produce a suitable *biometric sample(s)* (3.3.21) in accordance with the defined policy

Note 1 to entry: In addition to the *biometric capture process* (3.5.2), a **biometric acquisition process** may include segmentation, quality control and other pre-processing steps.

Note 2 to entry: A **biometric acquisition process** may produce multiple *biometric samples* (3.3.21) from a single *biometric capture* (3.6.3), where each *biometric sample* (3.3.21) is attributable to a single *biometric characteristic* (3.1.2). For example, (1) four fingerprints in a slap image, (2) three segmented face samples of the three people in a captured photograph.

Note 3 to entry: The policy defines the end point of the **biometric acquisition process**.

3.5.2
biometric capture process
series of actions undertaken to affect a *biometric capture* (3.6.3)

EXAMPLE To obtain an International Civil Aviation Organisation (ICAO) compliant passport photograph, the *biometric capture subject* (3.7.3) will have to undertake a number of steps e.g. remove glasses, look directly at the camera and not smiling etc. These steps are the **biometric capture process**

Note 1 to entry: Not all **biometric capture processes** result in a *biometric capture* (3.6.3).

Note 2 to entry: The **biometric capture process** may involve a single *biometric capture device* (3.4.1) or may be distributed over time and space in such a way that there is no single definable *biometric capture device* (3.4.1).

3.5.3
biometric enrolment
DEPRECATED: registration
act of creating and storing a *biometric enrolment data record* (3.3.10) in accordance with an enrolment policy

Note 1 to entry: Registration has a different meaning in the signal processing community and its use is therefore deprecated in *biometrics* (3.1.3) in favour of enrolment.

Note 2 to entry: Enrolment in a *biometric system* (3.2.3) might, in some cases, not involve storage of *biometric data* (3.3.6), for example, when *biometric data* (3.3.6) from an enrolee cannot be acquired.

3.5.4
biometric feature extraction
process applied to a *biometric sample* (3.3.21) with the intent of isolating and outputting repeatable and distinctive numbers or labels which can be compared to those extracted from other *biometric samples* (3.3.21)

Note 1 to entry: The creation of filters to be applied to *biometric samples* (3.3.21) is not **biometric feature extraction**, however, the application of filters to *biometric samples* (3.3.21) may be. Therefore, for example, the creation of eigenfaces is not **biometric feature extraction**.

Note 2 to entry: Repeatable implies low variation between outputs generated from *biometric samples* (3.3.21) of the same *biometric data subject* (3.7.5).

Note 3 to entry: Distinctive implies high variation between outputs generated from *biometric samples* (3.3.21) of different *biometric data subjects* (3.7.5).

Note 4 to entry: **Biometric feature extraction** may fail.

Note 5 to entry: **Biometric feature extraction** may be applied to an *intermediate biometric sample* (3.3.30).

3.5.5
biometric reference adaptation
automatic incremental updating of a *biometric reference* (3.3.16)

Note 1 to entry: **Biometric reference adaptation** may be used to improve performance (e.g. adapting the reference to take account of variability of an individual's *biometric characteristics* (3.1.2) and to mitigate performance degradation (e.g. due to changes in *biometric characteristics* (3.1.2) over time).

3.5.6
biometric search
examine a *biometric reference database* (3.3.17) against a *biometric probe* (3.3.14) to return either a *biometric candidate list* (3.3.5) or a *comparison decision* (3.3.26) that the *biometric probe* (3.3.14) does or does not *match* (3.3.31) with one or more *biometric references* (3.3.16)

Note 1 to entry: Output of the *biometric candidate list* (3.3.5) or the *comparison decision* (3.3.26) implies implementation of a policy.

Note 2 to entry: The *biometric reference database* (3.3.17) need not contain *biometric data* (3.3.6) from multiple *biometric data subjects* (3.7.5).

3.5.7
comparison
DEPRECATED: match (noun) (deprecated as a synonym for comparison)
DEPRECATED: matching (noun) (deprecated as a synonym for comparison)
estimation, calculation or measurement of similarity or dissimilarity between *biometric probe(s)* (3.3.14) and *biometric reference(s)* (3.3.16)

3.5.8
enrol
create and store a *biometric enrolment data record* (3.3.10) in accordance with the *biometric enrolment* (3.5.3) policy

3.5.9
intermediate biometric sample processing
any manipulation of a *biometric sample* (3.3.21) that does not produce *biometric features* (3.3.11)

EXAMPLE Examples of **intermediate biometric sample processing** include cropping, down-sampling, compression, conversion to data interchange formats standard and image enhancement.

3.5.10
one-to-one comparison
process in which *biometric probe(s)* (3.3.14) from one *biometric data subject* (3.7.5) is compared to *biometric reference(s)* (3.3.16) from one *biometric data subject* (3.7.5) to produce a *comparison score* (3.3.27)

Note 1 to entry: In the case of a *multi-modal* (3.2.6) *biometric system* (3.2.3), the *biometric probe* (3.3.14) and the *biometric reference* (3.3.16) may contain multiple *biometric modes* (3.2.5).

Note 2 to entry: Some one-to-one comparison algorithms, i.e. those using score normalization, cohort models or likelihood-ratios, may require comparisons of the *biometric probe* (3.3.14) from one *biometric data subject* (3.7.5) to *biometric references* (3.3.16) from multiple *biometric data subjects* (3.7.5). Nevertheless the *comparison score* (3.3.27) generated refers to the similarity between *biometric probe(s)* (3.3.14) of one *biometric data subject* (3.7.5) and a *biometric reference* (3.3.16) of one *biometric data subject* (3.7.5); therefore the process is considered a one-to-one comparison.

3.5.11
one-to-many comparison
DEPRECATED: one-to-few
process in which *biometric probe(s)* (3.3.14) of one *biometric data subject* (3.7.5) is compared against the *biometric references* (3.3.16) of more than one *biometric data subject* (3.7.5) to return a set of *comparison scores* (3.3.27)

Note 1 to entry: The term "compared" refers to *comparison* (3.5.7) in the *biometric* (3.1.1) sense.

3.5.12
one-to-many search
process in which *biometric probe(s)* (3.3.14) of one *biometric data subject* (3.7.5) is searched against the *biometric references* (3.3.16) of more than one *biometric data subject* (3.7.5) to return a *biometric candidate list* (3.3.5) or a *comparison decision* (3.3.26)

Note 1 to entry: The term "searched", in the above definition, refers to *biometric search* (3.5.6).

Note 2 to entry: Output of a *biometric candidate list* (3.3.5) or the *comparison decision* (3.3.26) implies implementation of a policy.

3.5.13
re-enrolment
process of establishing a new *biometric reference* (3.3.16) for a *biometric data subject* (3.7.5) already *enrolled* (3.5.8) in the *biometric enrolment database* (3.3.9)

Note 1 to entry: **Re-enrolment** requires new *captured biometric sample(s)* (3.3.25).

Note 2 to entry: For example, **re-enrolment** may be required as a result of performance degradation due to major changes in the system or *biometric characteristics* (3.1.2).

3.5.14
threshold (verb)
filter (verb)
eliminate *biometric reference identifier(s)* (3.3.19) associated with *biometric reference(s)* (3.3.16) and/or identifiers for *biometric probe(s)* (3.3.14) that have failed to attain a level of any type of score

Note 1 to entry: Score can be quality score, *comparison score* (3.3.27), etc.

3.6 Interacting terms

3.6.1
acceptable biometric capture attempt
capture attempt (3.6.8) that fulfils the requirements of a *biometric capture process* (3.5.2)

Note 1 to entry: Requirements of a *biometric capture process* (3.5.2) may be determined by the policy settings for system and subject behaviour.

3.6.2
acquire
successfully complete a *biometric acquisition process* (3.5.1)

3.6.3
biometric capture
obtain and record, in a retrievable form, signal(s) of *biometric characteristic(s)* (3.1.2) directly from individual(s), or from representation(s) of *biometric characteristic(s)* (3.1.2)

Note 1 to entry: Representation' is used in the natural language sense, e.g. a photograph.

Note 2 to entry: Retrievable' refers to the record and not the original signal.

Note 3 to entry: A signal can be generated by the *biometric characteristic* (3.1.2) or generated elsewhere and affected by the *biometric characteristic* (3.1.2). For example, face illuminated by incident light.

3.6.4
biometric claim
claim that a *biometric capture subject* (3.7.3) is or is not the bodily source of a specified or unspecified *biometric reference* (3.3.16)

Note 1 to entry: A **biometric claim** can be made by any *user* (3.7.20) of the *biometric system* (3.2.3).

Note 2 to entry: The phrase "claim of identity" is often used to label this concept.

Note 3 to entry: Claims may be positive – i.e. that the *biometric capture subject* (3.7.3) is *enrolled* (3.5.8); negative – i.e. that the *biometric capture subject* (3.7.3) is not *enrolled* (3.5.8), specific – i.e. that the *biometric capture subject* (3.7.3) is or is not *enrolled* (3.5.8) as a specified *biometric enrolee* (3.7.6); or non-specific – i.e. that the *biometric capture subject* (3.7.3) is or is not among the set or subset of *biometric enrolees* (3.7.6).

Note 4 to entry: **Biometric claims** are not necessarily made by the *biometric capture subject* (3.7.3).

Note 5 to entry: The *biometric reference* (3.3.16) could be on a database, card or distributed throughout a network.

Note 6 to entry: The **biometric claim** must fall within the *biometric system* (3.2.3) boundary.

3.6.5
biometric false acceptance
error of accepting a *biometric claim* (3.6.4) that should have been rejected in accordance with an authorative statement on the origin of the *biometric probe* (3.3.14) and the *biometric reference* (3.3.16)

3.6.6
biometric false rejection
error of rejecting a *biometric claim* (3.6.4) that should have been accepted in accordance with an authorative statement on the origin of the *biometric probe* (3.3.14) and the *biometric reference* (3.3.16)

3.6.7
biometric presentation
interaction of the *biometric capture subject* (3.7.3) and the *biometric capture subsystem* (3.2.1) to obtain a signal from a *biometric characteristic* (3.1.2)

Note 1 to entry: The *biometric capture subject* (3.7.3) may not be aware that a signal from a *biometric characteristic* (3.1.2) is being captured.

3.6.8
capture attempt
activity with the intent of producing a *captured biometric sample* (3.3.25)

Note 1 to entry: The **capture attempt** is the interface between the presentation by the *biometric capture subject* (3.7.3) and the action of the *biometric capture subsystem* (3.2.1).

Note 2 to entry: The "activity" taken may be on the part of the *biometric capture subsystem* (3.2.1) or the *biometric capture subject* (3.7.3).

3.6.9
capture task
prescribed set of *biometric capture subject* (3.7.3) behaviours in a *capture attempt* (3.6.8)

3.6.10
capture transaction
one or more *capture attempts* (3.6.8) with the intent of acquiring all of the *biometric data* (3.3.6) from a *biometric capture subject* (3.7.3) necessary to produce either a *biometric reference* (3.3.16) or a *biometric probe* (3.3.14)

3.6.11
cognizant presentation
presentation made with the *biometric capture subject's* (3.7.3) awareness

3.6.12
conformant capture attempt
actions that comply with the *capture task* (3.6.9)

3.6.13
cooperative presentation
presentation by a *cooperative biometric capture subject* (3.7.11)

Note 1 to entry: The *cooperative biometric capture subject* (3.7.11) might be untrained and perform the *biometric capture task* (3.6.9) poorly or incorrectly. Therefore, a **cooperative presentation** may not be a *conformant capture attempt* (3.6.12).

3.6.14
negative biometric claim
assertion that a *biometric capture subject* (3.7.3) is not the source of specified or unspecified *biometric reference(s)* (3.3.16) in a *biometric reference database* (3.3.17)

Note 1 to entry: Specified means there is a non-biometric input, such as a PIN, name or ID number, pointing to particular *biometric reference(s)* (3.3.16). Unspecified means there is no such non-biometric input provided.

3.6.15
non-conformant capture attempt
interactions of the *biometric capture subject* (3.7.3) and the *biometric capture subsystem* (3.2.1) that does not comply with the *capture task* (3.6.9)

3.6.16
indifferent presentation
presentation in which the *biometric capture subject* (3.7.3) is unconcerned that the *biometric capture process* (3.5.2) is occurring

Note 1 to entry: In an **indifferent presentation**, the *biometric capture subject* (3.7.3) is behaving neither cooperatively nor uncooperatively.

3.6.17
positive biometric claim
assertion that a *biometric capture subject* (3.7.3) is the source of specified or unspecified *biometric reference(s)* (3.3.16) in a *biometric reference database* (3.3.17)

Note 1 to entry: Specified means there is a non-biometric input, such as a PIN, name or ID number, pointing to particular *biometric reference(s)* (3.3.16). Unspecified means there is no such non-biometric input provided.

3.6.18
unacceptable capture attempt
capture attempt (3.6.8) that does not fulfil the requirements of a *biometric capture process* (3.5.2)

Note 1 to entry: Requirements of a *biometric capture process* (3.5.2) may be determined by the policy settings for the *biometric capture subsystem* (3.2.1) and the *biometric capture subject's* (3.7.3) behaviour.

3.6.19
uncooperative presentation
presentation by an *uncooperative biometric capture subject* (3.7.19)

Note 1 to entry: **Uncooperative presentation** may or may not be a *conformant capture attempt* (3.6.12).

Note 2 to entry: To be uncooperative, the *biometric capture subject* (3.7.3) must be aware that *biometric data* (3.3.6) is being collected.

3.6.20
verification attempt
biometric claim (3.6.4) and *capture attempt(s)* (3.6.8) that together provide the inputs for *comparison(s)* (3.5.7)

Note 1 to entry: The term *comparison* (3.5.7) refers to comparison in the *biometric* (3.1.1) sense.

3.6.21
verification transaction
one or more *verification attempts* (3.6.20) resulting in resolution of a *biometric claim* (3.6.4)

3.6.22
non-cognizant presentation
presentation made without the *biometric capture subject's* (3.7.3) awareness

Note 1 to entry: *Biometric capture subject* (3.7.3) may or may not be subversive.

Note 2 to entry: *Biometric capture subject* (3.7.3) may be aware of the general existence of *biometric systems* (3.2.3), but is unaware of the *biometric capture attempt* (3.6.8) of the system of interest.

3.6.23
capture subject training
instruction to an individual on system policy and required behaviour for submitting a *biometric sample* (3.3.21) and completing transactions.

Note 1 to entry: Instruction can be provided prior to or during the interaction of the *biometric capture subject* (3.7.3) with the system.

Note 2 to entry: Training can be through any of assorted methods, such as a human instructor, computer-based instruction, video presentation, printed text, or audio/visual feedback.

Note 3 to entry: Training can include instruction on eligibility, efficiency, security and timeliness.

3.6.24
capture subject habituation
degree of familiarity of a *biometric capture subject* (3.7.3) with the *biometric capture process* (3.5.2)

Note 1 to entry: A *biometric capture subject* (3.7.3) with substantial familiarity with the *biometric capture process* (3.5.2) is referred to as a *habituated capture subject* (3.7.24).

Note 2 to entry: Habituation may be acquired through system use or observation of use by others.

3.6.25
biometric presentation attack
presentation to the *biometric capture subsystem* (3.2.1) with the goal of interfering with the operation of the *biometric system* (3.2.3)

Note 1 to entry: **Biometric presentation attack**s can be implemented through a number of methods, e.g. artefact, mutilations, replay, etc.

Note 2 to entry: **Biometric presentation attack**s may have a number of goals, e.g. impersonation or not being recognized.

Note 3 to entry: *Biometric systems* (3.2.3) may not be able to differentiate between presentations with the goal of interfering with the systems' operation and non-conformant presentations.

3.6.26
biometric capture avoidance attack
deliberate action to elude interactions with *biometric systems* (3.2.3)

Note 1 to entry: A **biometric capture avoidance attack** is characterized by the deliberate circumvention of the *biometric capture subsystem* (3.2.1) by the *biometric capture subject* (3.7.3) with the aim of not having a signal captured.

3.6.27
biometric distortion attack
presentation of deliberately altered *biometric characteristics* (3.1.2)

3.6.28
biometric concealment attack
deliberately not revealing one's own *biometric characteristics* (3.1.2) while interacting with a biometric sensor

Note 1 to entry: No avoidance of the *biometric capture subsystem* (3.2.1) occurs in this attack.

3.6.29
biometric impostor attack
presentation of *biometric characteristics* (3.1.2) to impersonate another individual

3.6.30
cooperative
actively working in accordance with stated directions with the objective of successful biometric operations

Note 1 to entry: Successful biometric operation might result even in absence of cooperation.

Note 2 to entry: Does not apply to *biometric capture subjects* (3.7.3) or *biometric presentations* (3.6.7) in covert environments.

Note 3 to entry: Determination of **cooperative** requires interpretation.

Note 4 to entry: A *cooperative biometric capture subject* (3.7.11) might be subversive, just as a *user* (3.7.20) who is not cooperative is not necessarily subversive.

3.6.31
conformant
meeting required standards and policies

Note 1 to entry: Applied to *biometric presentations* (3.6.7), *biometric data* (3.3.6) and *biometric capture subject* (3.7.3).

3.6.32
cognizant
aware
biometric capture subject's (3.7.3) knowledge of the existence of a *biometric capture process* (3.5.2)

Note 1 to entry: This term can be applied to *biometric presentations* (3.6.7) or *biometric capture subjects* (3.7.3).

3.7 Personnel terms

3.7.1
biometric applicant
individual seeking to be *enrolled* (3.5.8) in a *biometric enrolment database* (3.3.9)

Note 1 to entry: **Biometric applicant** may or may not already be *enrolled* (3.5.8).

3.7.2
biometric attendant
agent of the *biometric system operator* (3.7.8) who directly interacts with the *biometric capture subject* (3.7.3)

EXAMPLE An immigration officer supervising a *biometric capture process* (3.5.2) and taking action on the *comparison decision* (3.3.26).

3.7.3
biometric capture subject
individual who is the subject of a *biometric capture process* (3.5.2)

Note 1 to entry: The individual remains a **biometric capture subject** only during the *biometric capture process* (3.5.2)

3.7.4
biometric characteristics examiner
individual with authority to assess *biometric characteristics* (3.1.2) and who does so for the purpose of resolving a *biometric claim* (3.6.4)

3.7.5
biometric data subject
individual whose individualized *biometric data* (3.3.6) is within the *biometric system* (3.2.3)

Note 1 to entry: The intent of the word "individualized" is to distinguish **biometric data subjects** from those whose aggregated data was used in the creation of the *biometric recognition* (3.1.3) algorithm. Examples of individuals contributing *biometric data* (3.3.6) who are not **biometric data subjects** include those who contributed to a Universal Background Model in speaker recognition systems, or who contributed to the creation of an eigenface basis set in a facial recognition system.

3.7.6
biometric enrolee
biometric data subject (3.7.5) whose *biometric data* (3.3.6) is held in a *biometric enrolment database* (3.3.9)

3.7.7
biometric operational personnel
individuals, other than the *biometric capture subjects* (3.7.3), who take an active role in the operation of the *biometric system* (3.2.3)

3.7.8
biometric system operator
person or organization who executes policies and procedures in the administration of a *biometric system* (3.2.3)

3.7.9
biometric system owner
person or organization with overall accountability for the acquisition, implementation and operation of the *biometric system* (3.2.3)

3.7.10
claimant
individual making a claim that can be verified biometrically

Note 1 to entry: The claimant need not be the *biometric data subject* (3.7.5).

3.7.11
cooperative biometric capture subject
biometric capture subject (3.7.3) motivated to achieve a successful completion of the *biometric acquisition process* (3.5.1)

Note 1 to entry: The **cooperative biometric capture subject** may be subversive or non-subversive.

3.7.12
biometric subversive concealer
subversive *biometric capture subject* (3.7.3) who attempts to avoid being matched to their own *biometric reference* (3.3.16)

3.7.13
biometric impostor
subversive *biometric capture subject* (3.7.3) who performs a *biometric impostor attack* (3.6.29)

Note 1 to entry: COED defines impostor as person who assumes a false identity in order to deceive or defraud.

Note 2 to entry: COED defines impersonate as pretend to be (another person) for entertainment or fraud.

3.7.14
indifferent biometric capture subject
biometric capture subject (3.7.3) who is unconcerned with the achievement of a successful *biometric acquisition process* (3.5.1)

Note 1 to entry: This implies the *biometric capture subject* (3.7.3) is neither cooperative nor uncooperative.

3.7.15
non-subversive biometric capture subject
biometric capture subject (3.7.3) who does not attempt to subvert the correct and intended system policy of the *biometric capture subsystem* (3.2.1)

3.7.16
non-subversive user
user (3.7.20) of a *biometric system* (3.2.3) who does not attempt to subvert the correct and intended system policy

3.7.17
subversive biometric capture subject
biometric capture subject (3.7.3) who attempts to subvert the correct and intended policy of the biometric capture subsystem (3.2.1)

3.7.18
subversive user
user (3.7.20) of a *biometric system* (3.2.3) who attempts to subvert the correct and intended system policy

EXAMPLE An operator who lets unsanctioned subjects through, a *user* (3.7.20) who initiates a denial of service attack, an administrator who allows unsanctioned function creep and a *biometric capture subject* (3.7.3) who impersonates an *enrolled* (3.5.8) *user* (3.7.20).

3.7.19
uncooperative biometric capture subject
biometric capture subject (3.7.3) motivated to not achieve a successful *biometric acquisition process* (3.5.1)

Note 1 to entry: The intent of the **uncooperative biometric capture subject** is either not to interact, or interact improperly, with the *biometric capture subsystem* (3.2.1).

3.7.20
user (of a biometric system)
DEPRECATED: end user
any person or organization interacting in any way with a *biometric system* (3.2.3)

Note 1 to entry: When discussing a particular class of users involved with *biometric systems* (3.2.3), the specific term for that class should be used. For example, those users whose *biometric data* (3.3.6) is being collected should be referred to as *biometric capture subjects* (3.7.3).

3.7.21
biometric concealer
subversive *biometric capture subject* (3.7.3) who performs a *biometric concealment attack* (3.6.28).

3.7.22
biometric avoider
subversive biometric capture subject (3.7.3) who performs a biometric capture avoidance attack (3.6.26).

Note 1 to entry: An avoider can bypass a *biometric system* (3.2.3) through any form of social engineering (bribery, for example).

3.7.23
biometric distorter
subversive *biometric capture subject* (3.7.3) who performs a *biometric distortion attack* (3.6.27)

3.7.24
habituated capture subject
biometric capture subject (3.7.3) with substantial familiarity with the biometric capture process (3.5.2)

3.7.25
non-habituated capture subject
biometric capture subject (3.7.3) without substantial familiarity with the biometric capture process (3.5.2)

3.8 Application terms

3.8.1
authentication
the act of proving or showing to be of undisputed origin or veracity

Note 1 to entry: Use of this term as a synonym for *biometric verification* (3.8.3) or *biometric identification* (3.8.2) is deprecated; the term *biometric recognition* (3.1.3) is preferred.

Note 2 to entry: This term has been used in *biometrics* (3.1.3) as a synonym primarily for: *biometric verification* (3.8.3) application, *biometric verification* (3.8.3) function, but also as a synonym for *biometric identification* (3.8.2) application and *biometric identification* (3.8.2) function.

3.8.2
biometric identification
process of searching against a *biometric enrolment database* (3.3.9) to find and return the *biometric reference identifier(s)* (3.3.19) attributable to a single individual

Note 1 to entry: Use of the term “authentication” as a substitute for **biometric identification** is deprecated.

3.8.3
biometric verification
process of confirming a *biometric claim* (3.6.4) through *biometric comparison* (3.5.7)

Note 1 to entry: Use of the term "authentication" as a substitute for **biometric verification** is deprecated.

3.8.4
duplicate biometric enrolment check
biometric identification (3.8.2) check that may be performed as a part of the *biometric enrolment* (3.5.3) process to ascertain the existing enrolment status of *biometric data subject* (3.7.5)

3.8.5
identify
biometric search (3.5.6) against a *biometric enrolment database* (3.3.9) to find and return the *biometric reference identifier(s)* (3.3.19) attributable to a single individual

3.8.6
verify
confirm a *biometric claim* (3.6.4) through *biometric comparisons* (3.5.7)

Note 1 to entry: It is understood that, in general, *biometric claims* (3.6.4) can neither be proven nor be refuted with certainty.

3.9 Performance terms

3.9.1
biometric mated comparison trial
comparison (3.5.7) of a *biometric probe* (3.3.14) and a *biometric reference* (3.3.16) from the same *biometric capture subject* (3.7.3) and the same *biometric characteristic* (3.1.2) as part of a performance test

Note 1 to entry: **Biometric mated comparison trials** have historically been referred to as "genuine trials", however, the term "genuine" historically implied an intent on the part of the *biometric data subject* (3.7.5). Ultimately the trial has nothing to do with the intention of the *biometric capture subject* (3.7.3).

3.9.2
biometric non-mated comparison trial
comparison (3.5.7) of a *biometric probe* (3.3.14) and a *biometric reference* (3.3.16) from different *biometric data subjects* (3.7.5) as part of a performance test

Note 1 to entry: **Biometric non-mated comparison trials** have historically been referred to as "impostor trials" however they do not accurately model operational system behavior in the presence of impostors.

Note 2 to entry: A set of **biometric non-mated comparison trials** need not contain all possible *comparisons* (3.5.7) of *biometric probes* (3.3.14) and *biometric references* (3.3.16) from different *biometric capture subjects* (3.7.3).

3.9.3
failure to acquire
FTA
failure to accept for subsequent *comparison* (3.5.7) the output of a *biometric capture process* (3.5.2), a *biometric sample* (3.3.21) of the *biometric characteristic* (3.1.2) of interest

Note 1 to entry: Acceptance of the output of a *biometric capture process* (3.5.2) for subsequent *comparison* (3.5.7) will depend on policy. Failure to acquire includes *failure to capture* (3.9.5).

Note 2 to entry: Other possible causes of **failure to acquire** include poor *biometric sample* (3.3.21) quality, algorithmic deficiencies and *biometric characteristics* (3.1.2) outside the range of the system.

3.9.4
failure-to-acquire rate
FTAR
proportion of a specified set of *biometric acquisition processes* (3.5.1) that were *failures to acquire* (3.9.3)

Note 1 to entry: The results of the *biometric acquisition processes* (3.5.1) may be *biometric probes* (3.3.14) or *biometric references* (3.3.16).

Note 2 to entry: The experimenter specifies which *biometric probe* (3.3.14) (or *biometric reference* (3.3.16)) acquisitions are in the set, as well as the criteria for deeming a *biometric acquisition process* (3.5.1) has failed.

Note 3 to entry: The proportion is the number of processes that failed divided by the total number of *biometric acquisition processes* (3.5.1) within the specified set.

3.9.5
failure to capture
FTC
failure of the *biometric capture process* (3.5.2) to produce a *captured biometric sample* (3.3.25) of the *biometric characteristic* (3.1.2) of interest

Note 1 to entry: The decision as to whether or not a *biometric sample* (3.3.21) has been captured depends on system policy, for example, one system may use a low-quality fingerprint whereas another might declare it a **failure to capture**.

3.9.6
failure to enrol
FTE
failure to create and store a *biometric enrolment data record* (3.3.10) for an eligible *biometric capture subject* (3.7.3), in accordance with a *biometric enrolment* (3.5.3) policy

Note 1 to entry: Not enrolling someone ineligible to *enrol* (3.5.8) is not a **failure to enrol.**

3.9.7
failure-to-enrol rate
FTER
proportion of a specified set of *biometric enrolment* (3.5.3) transactions that resulted in a *failure to enrol* (3.9.6)

Note 1 to entry: Basing the denominator on the number of *biometric enrolment* (3.5.3) transactions may result in a higher value than basing it on the number of *biometric capture subjects* (3.7.3).

Note 2 to entry: If the FTER is to measure solely transactions that fail to complete due to quality of the submitted *biometric data* (3.3.6) the denominator should not include transactions that fail due to non-biometric reasons (i.e. lack of eligibility due to age or citizenship).

3.9.8
false match
comparison (3.5.7) decision of *match* (3.3.31) for a *biometric probe* (3.3.14) and a *biometric reference* (3.3.16) that are from different *biometric capture subjects* (3.7.3)

Note 1 to entry: It is recognized that this definition considers the **false match** at the subject level only, and not at the *biometric characteristic* (3.1.2) level. Sometimes a *comparison* (3.5.7) may be made between a *biometric probe* (3.3.14) and a *biometric reference* (3.3.16) from different *biometric characteristics* (3.1.2) of a single *biometric capture subject* (3.7.3). In some of these cases — for example, when comparing Galton ridges of different fingers of the same *biometric data subject* (3.7.5) — a *comparison decision* (3.3.26) of *match* (3.3.31) might be considered to be an error, while in other cases — for example, when comparing a mispronounced pass-phrase in text-dependent speaker recognition — a *comparison decision* (3.3.26) of *match* (3.3.31) might be considered to be correct.

3.9.9
false match rate
FMR
proportion of the completed *biometric non-mated comparison trials* (3.9.2) that result in a false *match* (3.9.8)

Note 1 to entry: The value computed for the **false match rate** will depend on *thresholds* (3.3.36), and other parameters of the *comparison* (3.5.7) process, and the protocol defining the *biometric non-mated comparison trials* (3.9.2).

Note 2 to entry: *Comparisons* (3.5.7) between:

— identical twins;

— different, but related *biometric characteristics* (3.1.2) from the same individual, such as left and right hand topography will need proper consideration (see ISO/IEC 19795-1).

Note 3 to entry: "Completed" refers to the computational processes required to make a *comparison decision* (3.3.26), i.e. failures to decide are excluded.

3.9.10
false non-match
comparison decision (3.3.26) of "non-match" for a *biometric probe* (3.3.14) and a *biometric reference* (3.3.16) that are from the same *biometric capture subject* (3.7.3) and of the same *biometric characteristic* (3.1.2)

Note 1 to entry: There may need to be consideration on how much non-conformance to system policy on the part of the *biometric capture subject* (3.7.3) is tolerated before the probe *biometric sample* (3.3.21) and the *biometric reference* (3.3.16) are deemed to be of different *biometric characteristics* (3.1.2).

3.9.11
false non-match rate
FNMR
proportion of the completed *biometric mated comparison trials* (3.9.1) that result in a *false non-match* (3.9.10)

Note 1 to entry: The value computed for the **false non-match rate** will depend on *thresholds* (3.3.36), and other parameters of the *comparison* (3.5.7) process, and the protocol defining the *biometric mated comparison trials* (3.9.1).

Note 2 to entry: "Completed" refers to the computational processes required to make a *comparison decision* (3.3.26), i.e. failures to decide are excluded.

3.9.12
comparison trial
single *biometric probe* (3.3.14) to *biometric reference* (3.3.16) *comparison* (3.5.7) in a test of performance

3.9.13
quality score
quantitative value of the fitness of a *biometric sample* (3.3.21) to accomplish or fulfil the *comparison decision* (3.3.26)

3.9.14
quality
a measure of the fitness of a *biometric sample* (3.3.21) to accomplish or fulfil the *biometric comparison decision* (3.3.26)

Note 1 to entry: **Quality** is a measure of *biometric utility* (3.9.16).