INTERNATIONAL STANDARD

ISO/IEC 2382-37

First edition
2012-12-15

Information technology — Vocabulary —

Part 37: Biometrics

Technologies de l'information — Vocabulaire —

Partie 37: Biométrie

Reference number
ISO/IEC 2382-37:2012(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 2382-37 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 37, *Biometrics*.

ISO/IEC 2382 consists of a total of 37 parts, under the general title *Information technology — Vocabulary.*

Introduction

The main purpose of this part of ISO/IEC 2382 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 sub-fields.

This part of ISO/IEC 2382 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 in **bold** are defined in this document. Words that are not in bold 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 (COD), 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.

EXAMPLE
candidate
<biometrics> **biometric reference identifier** of a **biometric reference** in the **biometric reference database** determined to be similar to the **biometric probe**

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 should be 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 might be omitted completely.

The terms in this part of ISO/IEC 2382 are listed in a systematic order under a number of general headings.

The layout follows the directions given in ISO 10241. 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)

To clarify in which grammatical context a term is defined the following indicators are used: (n) for a noun, (v) for a verb and (adj) for an adjective.

The alphabetical index includes preferred and admitted terms.

Information technology — Vocabulary —

Part 37:
Biometrics

1 Scope

This part of ISO/IEC 2382 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 the scope of this part of ISO/IEC 2382.

Words in **bold** are defined in this document. Words that are not in bold 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 (COD), 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.

3 Biometric vocabulary

3.1 General concept terms

37.01.01
biometric (adj)
of or having to do with **biometrics**

NOTE The use of **biometric** as a noun, to mean for example, **biometric characteristic**, 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 mode** 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** recorded in my passport is a facial image.

37.01.02
biometric characteristic
biometric (deprecated)
biological and behavioural characteristic of an individual from which distinguishing, repeatable **biometric features** can be extracted for the purpose of **biometric recognition**

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.

NOTE 1 Biological and behavioural characteristics are physical properties of body parts, physiological and behavioural processes created by the body and combinations of any of these.

NOTE 2 Distinguishing does not necessarily imply individualization.

37.01.03
biometric recognition
biometrics
automated recognition of individuals based on their biological and behavioural characteristics

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

NOTE 2 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 **Biometric recognition** encompasses **biometric verification** and **biometric identification.**

NOTE 4 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 Biological and behavioural 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 Use of 'authentication' as a synonym for “**biometric verification** or **biometric identification**” is deprecated; the term **biometric recognition** is preferred.

3.2 Biometric system terms

37.02.01
biometric capture subsystem
biometric capture device(s) and any sub-processes required to execute a **biometric capture process**

EXAMPLE In some systems, converting a signal from a **biometric characteristic** to a **captured biometric sample** may include multiple components such as a camera, photographic paper, printer, digital scanner, ink and paper.

NOTE A **biometric capture subsystem** can consist of only a single **biometric capture device**.

37.02.02
biometric identification system
system that aims to perform **biometric identification**

37.02.03
biometric system
system for the purpose of the **biometric recognition** of individuals based on their behavioural and biological characteristics

NOTE A **biometric system** will contain both **biometric** and non-biometric components.

37.02.04
biometric verification system
system that aims to perform **biometric verification**

37.02.05
mode
combination of a **biometric characteristic** type, a sensor type and a processing method

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

NOTE 2 Determining what constitutes a single type of sensor, processing method or **biometric characteristic** will depend on convention. For example, current convention is that images of ridge patterns from both thumbs and fingers constitute a single **biometric characteristic** 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.

37.02.06
multi-modal
multiple in at least 2 out of 3 constituents of a **mode** in a single **biometric system**

NOTE Multiple implies difference in type.

3.3 Terms for data in biometric systems

37.03.01
anonymized biometric data record
biometric data record purposely disassociated from individual metadata

NOTE The **biometric data** within the **biometric data record** ultimately remains attributable to an individual.

37.03.02
biometric application database
database of **biometric data** and associated metadata developed from and supporting the operation of a **biometric application**

NOTE 1 The metadata may include transaction history; authorisations (e.g. age) of **biometric data subjects**; and archived **biometric data**.

NOTE 2 The term application includes the policies that govern the operation of the system and evidence of that operation.

37.03.03
biometric application decision
decision to perform an action at the application level based on the results of a **biometric** process

NOTE 1 The application decision may include more than a comparison process. For example, a **biometric capture process** may show that there are no characteristics to capture and a decision can be made on this before any **biometrics** are compared.

NOTE 2 **Biometric application decisions** can be made on the basis of complex policies involving both **biometric** and non-biometric data.

37.03.04
biometric candidate
biometric reference identifier of a **biometric reference** in the **biometric reference database** determined to be sufficiently similar to the **biometric probe** to warrant further analysis

37.03.05
biometric candidate list
set of zero, one or more **biometric candidates** that may be intermediate or final

NOTE 1 Intermediate **biometric candidate lists** may be produced by systems that use multi-pass **biometric identification**.

NOTE 2 **Biometric candidate lists** may or may not be ordered.

37.03.06
biometric data
biometric sample or aggregation of biometric samples at any stage of processing, e.g. **biometric reference**, **biometric probe**, **biometric feature** or **biometric property**

NOTE Biometric data need not be attributable to a specific individual, e.g. Universal Background Models.

37.03.07
biometric database
database of **biometric data record(s)**

37.03.08
biometric data record
data record containing **biometric data**

NOTE A **biometric data record** may include **non-biometric data**.

37.03.09
biometric enrolment database
database of **biometric enrolment data record(s)**

NOTE 1 A database of biometric data not attributable to biometric data subjects is a biometric database, but not a biometric enrolment database. e.g. a universal background model.

NOTE 2 The **biometric enrolment database** may, or may not contain the **biometric reference database**. Separation of the databases may be required due to security, privacy, legislation, architecture, performance, etc.

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

37.03.10
biometric enrolment data record
data record attributed to a **biometric data subject**, containing non-biometric data and associated with **biometric reference identifier**(s)

NOTE 1 Data can be updated after enrolment.

NOTE 2 The **biometric enrolment data record** will either contain biometric reference data record(s) or pointer(s) to biometric reference data record(s).

NOTE 3 The associated **biometric reference** may be NULL (for example, **biometric enrollee** lacks the **biometric characteristic** or **biometric capture** is pending).

37.03.11
biometric feature
numbers or labels extracted from **biometric samples** and used for comparison

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

NOTE 2 The use of this term should 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**.

NOTE 4 **Biometric features** may be extracted from an intermediate **biometric sample**.

NOTE 5 Filters applied to **biometric samples** 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**.

37.03.12
biometric identification decision
comparison decision as to whether a **biometric reference(s)** of a particular **biometric data subject** is in a **biometric reference database**

NOTE 1 Return of a **biometric candidate list** is not considered a **biometric identification decision**.

NOTE 2 A positive **biometric identification** process is inferred from the output of a **biometric reference identifier**.

37.03.13
biometric model
stored function generated from biometric data

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

NOTE 1 In most occasions the **biometric model** is a stored function which is dependent on the **biometric data subject**.

NOTE 2 The function may be determined through training.

NOTE 3 A **biometric model** may involve intermediate processing similar to **biometric feature extraction.**

37.03.14
biometric probe
biometric query
biometric sample or **biometric feature** set input to an algorithm for use as the subject of **biometric comparison** to a **biometric reference(s)**

NOTE 1 The term comparison refers to comparison in the biometric sense.

NOTE 2 The subject/object labeling in a comparison might be arbitrary. In some comparisons a **biometric reference** might be used as the subject of the comparison with other **biometric references** or incoming samples used as the objects of the comparisons. 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.

NOTE 3 Typically in a biometric comparison process, incoming biometric samples serve as the subject of comparison against objects stored as biometric references in a database.

37.03.15
biometric property
descriptive attributes of the **biometric data subject** estimated or derived from the **biometric sample** by automated means

EXAMPLE Fingerprints can be classified by the biometric properties of ridge-flow, i.e. arch, whorl, and loop types. In the case of facial recognition, this could be estimates of age or gender.

37.03.16
biometric reference
one or more stored **biometric samples**, **biometric templates** or **biometric models** attributed to a **biometric data subject** and used as the object of biometric comparison

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

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

NOTE 2 The subject/object labeling in a comparison might be arbitrary. In some comparisons a **biometric reference** might be used as the subject of the comparison with other **biometric references** or incoming samples used as the objects of the comparisons. 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.

37.03.17
biometric reference database
database of **biometric reference data records**

NOTE The **biometric reference database** may be a subset of the **biometric enrolment database**, or it may be a separate database. Separation of the databases may be required due to security, privacy, legislation, architecture, performance, etc.

37.03.18
biometric reference data record
indexed data record containing **biometric reference(s)**

NOTE There may not be a one to one correspondence between biometric reference data records and **biometric data subjects** e.g. a single **biometric data subject** 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**

37.03.19
biometric reference identifier
pointer to a **biometric reference data record** in the **biometric reference database**

37.03.20
biometric representation
biometric sample or **biometric feature** set

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

37.03.21
biometric sample
analog or digital representation of **biometric characteristics** prior to **biometric feature extraction**

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

37.03.22
biometric template
reference biometric feature **set**
set of stored biometric features comparable directly to probe biometric features

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

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

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

37.03.23
biometric verification decision
comparison decision determining the validity of a **biometric claim** in a **verification transaction**

37.03.24
biometric candidate score
comparison score for a **biometric candidate**

37.03.25
captured biometric sample
raw biometric sample (deprecated)
biometric sample resulting from a **biometric capture process**

37.03.26
comparison decision
determination of whether the **biometric probe(s)** and **biometric reference(s)** have the same **biometric** source, based on a **comparison score(s)**, a decision policy(ies) including a threshold, and possibly other inputs

NOTE A **match** is a positive comparison decision. A **non-match** is a negative comparison decision. A decision of "undetermined" may sometimes be given.

37.03.27
comparison score
matching score (deprecated)
numerical value (or set of values) resulting from a comparison

NOTE Higher does not necessarily mean more similar.

37.03.28
dissimilarity score
distance score
comparison score that decreases with similarity

37.03.29
fraudulent biometric enrolment data record
biometric enrolment data record created or modified for the purpose of supporting wrongful or criminal activity

NOTE Records that are inadvertently erroneous or created for test purposes are not considered fraudulent.

37.03.30
intermediate biometric sample
biometric sample resulting from intermediate **biometric sample** processing

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

37.03.31
match (n)
comparison decision stating that the **biometric probe(s)** and the **biometric reference** are from the same source

NOTE 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 process its use as a verb is deprecated in favour of compare.

37.03.32
mated (adj)
of or having to do with a paired **biometric probe** and **biometric reference** that are from the same **biometric characteristic** of the same **biometric data subject**

NOTE While '**match**' is the result of a **biometric comparison decision**, '**mated'** is a statement, based on non-biometric information, concerning the origin of the source of the **biometric probe** and the **biometric reference**.

37.03.33
non-match (n)
comparison decision stating that the **biometric probe(s)** and the biometric reference are not from the same source

37.03.34
non-mated (adj)
of or having to do with a paired **biometric probe** and **biometric reference** that are not from the same **biometric characteristic** of the same **biometric data subject**

NOTE While '**non-match**' is the result of a **biometric comparison decision**, '**non-mated'** is a statement, based on non-biometric information, concerning the origin of the source of the **biometric probe** and the **biometric reference**.

37.03.35
similarity score
comparison score that increases with similarity

37.03.36
threshold (n)
numerical value (or set of values) at which a decision boundary exists

37.03.37
unidentified biometric data
biometric data whose **biometric data subject** is currently unknown

3.4 Device terms

37.04.01
biometric capture device
device that collects a signal from a **biometric characteristic** and converts it to a **captured biometric sample**

NOTE 1 A signal can be generated by the **biometric characteristic** or generated elsewhere and affected by the **biometric characteristic**, for example, face illuminated by incident light.

NOTE 2 A device can be any piece of hardware (and supporting software and firmware).

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

3.5 Functioning terms

37.05.01
biometric acquisition process
biometric capture process and additional processing to attempt to produce a suitable **biometric sample(s)** in accordance with the defined policy

NOTE 1 In addition to the capture process, an acquisition process may include segmentation, quality control and other pre-processing steps.

NOTE 2 An acquisition process may produce multiple biometric samples from a single **biometric capture**, each **biometric sample** is attributable to a single **biometric characteristic**. For example, (1) four fingerprints in a slap image, (2) three segmented face samples of the three people in a captured photograph.

NOTE 3 The policy defines the end point of the acquisition process.

37.05.02
biometric capture process
collecting or attempting to collect a signal(s) from a **biometric characteristic(s),** or a representation(s) of a **biometric characteristic(s**,**)** and converting the signal(s) to a captured **biometric sample** set

NOTE 1 A signal can be generated by the **biometric characteristic** or generated elsewhere and affected by the biometric characteristic. For example, face illuminated by incident light.

NOTE 2 Each signal collected could stem from a different presentation.

NOTE 3 The **biometric capture process** may involve a single **biometric capture device**. In other systems the capture may be distributed over time and space in such a way that there is no single definable **biometric capture device**.

37.05.03
biometric enrolment
registration (deprecated)
act of creating and storing a **biometric enrolment data record** in accordance with an enrolment policy

NOTE Registration has a different meaning in the signal processing community and its use is therefore deprecated in biometrics in favour of enrolment

37.05.04
biometric feature extraction
process applied to a **biometric sample** with the intent of isolating and outputting repeatable and distinctive numbers or labels which can be compared to those extracted from other **biometric samples**

NOTE 1 The creation of filters to be applied to **biometric samples** is not **biometric feature extraction**, however the application of filters to **biometric samples** may be. Therefore, for example, the creation of eigenfaces is not **biometric feature extraction**.

NOTE 2 Repeatable implies low variation between outputs generated from **biometric samples** of the same biometric data subject.

NOTE 3 Distinctive implies high variation between outputs generated from **biometric samples** of different **biometric data subjects**.

NOTE 4 **Biometric feature extraction** may generate an error message or a NULL vector.

NOTE 5 **Biometric feature extraction** may be applied to an intermediate biometric sample.

37.05.05
biometric reference adaptation
automatic incremental updating of a **biometric reference**

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

37.05.06
biometric search
examine a **biometric reference database** against a **biometric probe** to return either a **biometric candidate list** or a **comparison decision** that the **biometric probe** does or does not match with one or more **biometric references**

NOTE 1 Output of the **biometric** candidate list or the comparison decision implies implementation of a policy.

NOTE 2 The biometric reference database need not contain biometric data from multiple biometric data subjects.

37.05.07
comparison
match (n) (deprecated as a synonym for comparison)
matching (n) (deprecated as a synonym for comparison)
estimation, calculation or measurement of similarity or dissimilarity between **biometric probe(s)** and **biometric reference(s)**

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

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

37.05.08
enrol
create and store a **biometric enrolment data record** in accordance with the **biometric enrolment** policy

37.05.09
intermediate biometric sample processing
any manipulation of a **biometric sample** that does not produce **biometric features**

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

37.05.10
one-to-one comparison
process in which **biometric probe(s)** from one **biometric data subject** is compared to **biometric reference(s)** from one biometric data subject to produce a comparison score.

NOTE 1 In the case of a multi-modal biometric system, the **biometric probe** and the **biometric reference** may contain multiple biometric modes.

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

37.05.11
one-to-many comparison
one-to-few (deprecated)
process in which **biometric probe(s)** of one **biometric data subject** is compared against the **biometric references** of more than one **biometric data subject** to return a set of **comparison scores**

NOTE The term “compared” refers to comparison in the **biometric** sense.

37.05.12
one-to-many search
process in which **biometric probe(s)** of one **biometric data subject** is searched against the **biometric references** of more than one **biometric data subject** to return a **candidate list** or a **comparison decision**

NOTE 1 The term “searched”, in the above definition, refers to **biometric search**.

NOTE 2 Output of a **candidate list** or the **comparison decision** implies implementation of a policy.

37.05.13
re-enrolment
process of establishing a new **biometric reference** for a **biometric data subject** already enrolled in the **biometric enrolment database**

NOTE 1 **Re-enrolment** requires new **captured biometric sample(s)**.

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

37.05.14
threshold (v)
filter(v)
eliminate **biometric reference identifier(s)** associated with **biometric reference(s)** and/or identifiers for **biometric probe(s)** that have failed to attain a level of any type of score

NOTE Score can be quality score, comparison score, etc.

3.6 Interacting terms

37.06.01
acceptable biometric capture attempt
capture attempt that fulfils the requirements of a **biometric capture process**

NOTE Requirements of a **biometric capture process** may be determined by the policy settings for system and subject behaviour.

37.06.02
acquire
successfully complete a **biometric** acquisition process

37.06.03
biometric capture
obtain and record, in a retrievable form, signal(s) of **biometric characteristic(s)** directly from individual(s), or from representation(s) of **biometric characteristic(s)**

NOTE 1 'Representation' is used in the natural language sense, e.g., a photograph.

NOTE 2 'Retrievable' refers to the record and not the original signal.

NOTE 3 A signal can be generated by the **biometric characteristic** or generated elsewhere and affected by the **biometric characteristic**. For example, face illuminated by incident light.

NOTE 4 Multiple **biometric characteristics** may be captured from a single individual or from multiple individuals.

37.06.04
biometric claim
claim that a **biometric capture subject** is or is not the bodily source of a specified or unspecified **biometric reference**

NOTE 1 A **biometric claim** can be made by any **user** of the **biometric system**.

NOTE 2 The phrase "claim of identity" is often used to label this concept.

NOTE 3 Claims may be positive – i.e. that the **biometric capture subject** is enrolled; negative – i.e. that the **biometric capture subject** is not enrolled; specific – i.e. that the **biometric capture subject** is or is not enrolled as a specified biometric enrollee; or non-specific – i.e. that the **biometric capture subject** is or is not among the set or subset of biometric enrollees.

NOTE 4 **Biometric claims** are not necessarily made by the biometric capture subject.

NOTE 5 The **biometric reference** could be on a database, card or distributed throughout a network.

NOTE 6 The **biometric claim** must fall within the **biometric system** boundary.

37.06.05
biometric false acceptance
error of accepting a **biometric claim** that should have been rejected in accordance with an authorative statement on the origin of the **biometric probe** and the **biometric reference**

37.06.06
biometric false rejection
error of rejecting a **biometric claim** that should have been accepted in accordance with an authorative statement on the origin of the **biometric probe** and the **biometric reference**

37.06.07
biometric presentation
interaction of the **biometric capture subject** and the **biometric capture subsystem** to obtain a signal from a **biometric characteristic**

NOTE The **biometric capture subject** may not be aware that a signal from a **biometric characteristic** is being captured.

37.06.08
capture attempt
activity with the intent of producing a **captured biometric sample**

NOTE 1 The **capture attempt** is the interface between the presentation by the **biometric capture subject** and the action of the **biometric capture subsystem**.

NOTE 2 The "activity" taken may be on the part of the **biometric capture subsystem** or the **biometric capture subject**.

37.06.09
capture task
prescribed set of **biometric capture subject** behaviours in a **capture attempt**

37.06.10
capture transaction
one or more **capture attempts** with the intent of acquiring all of the biometric data from a **biometric capture subject** necessary to produce either a **biometric reference** or a **biometric probe**

37.06.11
cognizant presentation
presentation made with the **biometric capture subject's** awareness

37.06.12
conformant capture attempt
actions that comply with the **capture task**

37.06.13
cooperative presentation
presentation by a **cooperative biometric capture subject**

NOTE 1 The **cooperative biometric capture subject** might be untrained, perform the **biometric capture task** poorly or incorrectly.

NOTE 2 **Cooperative presentation** may or may not be a **conformant capture attempt**.

37.06.14
negative biometric claim
assertion that a **biometric capture subject** is not the source of specified or unspecified **biometric reference(s)** in a **biometric reference database**

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

37.06.15
non-conformant capture attempt
actions that do not comply with the capture task

37.06.16
indifferent presentation
presentation in which the **biometric capture subject** is unconcerned that the **biometric capture process** is occurring

NOTE In an **indifferent presentation** the **biometric capture subject** is behaving neither cooperatively nor uncooperatively.

37.06.17
positive biometric claim
assertion that a **biometric capture subject** is the source of specified or unspecified **biometric reference(s)** in a **biometric reference database**

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

37.06.18
unacceptable capture attempt
capture attempt that does not fulfil the requirements of a **biometric capture process**

NOTE Requirements of a **biometric capture process** may be determined by the policy settings for the **biometric capture subsystem** and the **biometric capture subject's** behaviour.

37.06.19
uncooperative presentation
presentation by an **uncooperative biometric capture subject**

NOTE 1 **Uncooperative presentation** may or may not be a **conformant capture attempt**.

NOTE 2 To be uncooperative, the **biometric capture subject** must be aware that **biometric data** is being collected.

37.06.20
verification attempt
biometric claim and capture attempt(s) that together provide the inputs for comparison(s)

NOTE The term "comparison" refers to comparison in the biometric sense.

37.06.21
verification transaction
one or more **verification attempts** resulting in resolution of a **biometric claim**

3.7 Personnel terms

37.07.01
biometric applicant
individual seeking to be enrolled in a **biometric enrolment database**

NOTE **Biometric applicant** may or may not already be enrolled.

37.07.02
biometric attendant
agent of the biometric system operator who directly interacts with the **biometric capture subject**

EXAMPLE An immigration officer supervising **biometric capture process** and taking action on the comparison decision.

37.07.03
biometric capture subject
individual who is the subject of a **biometric capture process**

NOTE The individual remains a biometric capture subject only during the biometric capture process.

37.07.04
biometric characteristics examiner
individual with authority to assess **biometric characteristics** and who does so for the purpose of resolving a **biometric claim**

37.07.05
biometric data subject
individual whose individualized **biometric data** is within the **biometric system**

NOTE 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** algorithm. Examples of individuals contributing **biometric data** 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.

37.07.06
biometric enrollee
biometric data subject whose **biometric data** is held in a **biometric enrolment database**

37.07.07
biometric operational personnel
individuals, other than the **biometric capture subjects**, who take an active role in the operation of the **biometric system**

37.07.08
biometric system operator
person or organization who executes policies and procedures in the administration of a **biometric system**

37.07.09
biometric system owner
person or organization with overall accountability for the acquisition, implementation and operation of the **biometric system**

37.07.10
claimant
individual making a claim that can be verified biometrically

NOTE The claimant need not be the **biometric data subject.**

37.07.11
cooperative biometric capture subject
biometric capture subject motivated to achieve a successful completion of the **biometric acquisition process**

NOTE The **cooperative biometric capture subject** may be subversive or non-subversive.

37.07.12
identity concealer
subversive **biometric capture subject** who attempts to avoid being matched to their own **biometric reference**

37.07.13
impostor
subversive biometric capture subject who attempts to be matched to someone else's **biometric reference**

NOTE The COD defines impostor as a person who assumes a false identity in order to deceive or defraud[1].

37.07.14
indifferent biometric capture subject
biometric capture subject who is unconcerned with the achievement of a successful **biometric acquisition process**

NOTE This implies the **biometric capture subject** is neither cooperative nor uncooperative.

37.07.15
non-subversive biometric capture subject
biometric capture subject who does not attempt to subvert the correct and intended system policy of the **biometric capture subsystem**

37.07.16
non-subversive user
user of a **biometric system** who does not attempt to subvert the correct and intended system policy

37.07.17
subversive biometric capture subject
biometric capture subject who attempts to subvert the correct and intended policy of the **biometric capture subsystem**

37.07.18
subversive user
user of a **biometric system** who attempts to subvert the correct and intended system policy

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

37.07.19
uncooperative biometric capture subject
biometric capture subject motivated to not achieve a successful **biometric acquisition process**

NOTE The intent of the **uncooperative biometric capture subject** is either not to interact, or interact improperly, with the **biometric capture subsystem**.

37.07.20
user (of a biometric system)
end user (deprecated)
any person or organization interacting in any way with a **biometric system**

NOTE When discussing a particular class of users involved with **biometric systems**, the specific term for that class should be used. For example, those users whose **biometric data** is being collected should be referred to as **biometric capture subjects.**

3.8 Application terms

37.08.01
authentication
the act of proving or showing to be of undisputed origin or veracity

NOTE 1 Use of this term as a synonym for "**biometric verification** or **biometric identification**" is deprecated; the term **biometric recognition** is preferred.

NOTE 2 This term has been used in **biometrics** as a synonym primarily for: **biometric verification** application, **biometric verification** function, but also as a synonym for **biometric identification** application and **biometric identification** function.

37.08.02
biometric identification
process of searching against a **biometric enrolment database** to find and return the **biometric reference identifier(s)** attributable to a single individual

NOTE Use of the term "**authentication**" as a substitute for **biometric identification** is deprecated.

37.08.03
biometric verification
process of confirming a **biometric claim** through **biometric comparison**

NOTE 1 The term “verifying”, in the above definition, refers to verify (**biometrics**).

NOTE 2 Use of the term “authentication” as a substitute for **biometric verification** is deprecated.

37.08.04
duplicate biometric enrolment check
biometric identification check that may be performed as a part of the **enrolment process** to ascertain existing enrolment status of **biometric data subject**

37.08.05
identify
biometric search against a **biometric enrolment database** to find and return the **biometric reference identifier(s)** attributable to a single individual

37.08.06
verify
confirm a **biometric claim** through **biometric comparisons**

NOTE It is understood that, in general, biometric claims can neither be proven nor be refuted with certainty.

3.9 Performance terms

37.09.01
biometric mated comparison trial
comparison of a **biometric probe** and a **biometric reference** from the same **biometric data subject** and the same **biometric characteristic** as part of a performance test

NOTE **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**. Ultimately the trial has nothing to do with the intention of the **biometric capture subject**.”

37.09.02
biometric non-mated comparison trial
comparison of a biometric probe and a biometric reference from different biometric data subjects as part of a performance test

NOTE 1 **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 A set of **biometric non-mated comparison trials** need not contain all possible comparisons of **biometric probes** and **biometric references** from different **biometric capture subjects biometric characteristics**.

37.09.03
failure to acquire
failure to accept for subsequent comparison the output of a data capture process

NOTE 1 **Failure to acquire** occurs if the captured data does not meet system policy requirements for processing. **Failure to acquire** can only occur if there has been a successful data capture event. Otherwise the event is a **failure to capture.**

NOTE 2 Possible causes of **failure to acquire** include poor biometric sample quality, algorithmic deficiencies and **biometric characteristics** outside the range of the system.

37.09.04
failure-to-acquire rate (FTA)
proportion of a specified set of **biometric acquisition processes** that were **failures to acquire**