INTERNATIONAL STANDARD

ISO/IEC 2382-37

Third edition
2022-03

Information technology — Vocabulary —

Part 37: Biometrics

Technologies de l'information — Vocabulaire —

Partie 37: Biométrie

Информационные технологии — Словарь —

Часть 37: Часть 37: Биометрия

IECNORM.COM : Click to view the full PDF of ISO/IEC 2382-37:2022

Reference number
ISO/IEC 2382-37:2022(E)

© ISO/IEC 2022

IECNORM.COM : Click to view the full PDF of ISO/IEC 2382-37:2022

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2022

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

IECNORM.COM : Click to view the full PDF of ISO/IEC 2382-37:2022

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.

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 document 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 or www.iec.ch/members_experts/refdocs).

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. 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) or the IEC list of patent declarations received (see https://patents.iec.ch).

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

For an explanation of the voluntary nature of standards, 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 www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 37, *Biometrics*.

This third edition cancels and replaces the second edition (ISO/IEC 2382-37:2017), which has been technically revised.

The main changes are as follows:

- modifications to some of the terms published in the 2017 edition; and
- addition of new terms related to biometric systems (starting from 37.02.08), data in biometric systems (starting from 37.03.42), devices (37.04.02), interaction (starting from 37.06.33), personnel (starting from 37.07.26) and performance (starting from 37.09.23).

A list of all parts in the ISO/IEC 2382 series can be found on the ISO and IEC websites.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

IECNORM.COM : Click to view the full PDF of ISO/IEC 2382-37:2022

© ISO/IEC 2022 – All rights reserved

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 sub-fields.

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

The terms defined in this document are to be understood within the context of the subject field of biometrics. When terms exist in various subject fields, the relevant subject field is indicated in angle brackets.

Words that are written in italics are defined in this document. Words that are written in upright font 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 (COED), Thumb Index Edition (tenth edition, revised, 2002).

The numbering of all terms in this document begins with “37” to indicate the Subcommittee of Joint Technical Committee ISO/IEC JTC 1 that created the terms. This is consistent will all other parts of the ISO/IEC 2382 series. The subsequent numerical heading for each entry within this document (37.xx) represents the number of the highest-level category in the concept map in which the term primarily falls. This is consistent with “Systematic Order” as described in ISO 10241-1:2011, 5.1.2, in which the heading reflects the concept system. In the first edition of this document (ISO/IEC 2382-37:2012), the third numerical designator (37.xx.yy) was also consistent with “Systematic Order”, moving from most general to more specific terms within each highest-level category of the concept map. With the development of the current edition of this document, the decision was made to append the new terms in each category such that the numbering of the earlier terms inherited from the 2012 edition would not change. This implies that the third numerical designator is now in “Mixed Order” as described in ISO 10241-1:2011, 5.1.3.

So, terms are added to this document in batches for each updated version. These terms are added in alphabetical order. This ensures that the numbers allocated to a term remain the same and that they can be referred to consistently.

The terms in this document are listed 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)
- Deprecated term(s)
- Definition (mandatory)
- Example(s)
- Note(s) to entry

The alphabetical index includes preferred and admitted terms.

IECNORM.COM : Click to view the full PDF of ISO/IEC 2382-37:2022

IECNORM.COM : Click to view the full PDF of ISO/IEC 2382-37:2022

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. This document also reconciles variant terms in use in pre-existing International Standards on biometrics against the preferred terms, thereby clarifying the use of terms in this field.

This document does not cover 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.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at https://www.iso.org/obp
- IEC Electropedia: available at https://www.electropedia.org/

3.1 Terms related to general concepts

37.01.01
biometric, adj
of or having to do with *biometrics* (37.01.03)

Note 1 to entry: The use of biometric as a noun, to mean for example, *biometric characteristic* (37.01.02), 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* (37.02.05) 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.

Note 2 to entry: Since the late 19th century the terms 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.

IECNORM.COM : Click to view the full PDF of ISO/IEC 2382-37:2022

© ISO/IEC 2022 – All rights reserved

37.01.02
biometric characteristic
DEPRECATED biometric
biological and behavioural characteristic of an individual from which distinguishing, repeatable *biometric features* (37.03.11) can be extracted for the purpose of *biometric recognition* (37.01.03)

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.

37.01.03
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* (37.08.03) and *biometric identification* (37.08.02).

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 or biometric identification” is deprecated; the term biometric recognition is preferred.

3.2 Terms related to biometric systems

37.02.01
biometric capture subsystem
biometric capture devices (37.04.01) and any sub-processes required to execute a *biometric capture process* (37.05.02)

Note 1 to entry: In some *biometric systems* (37.02.03), converting a signal from a *biometric characteristic* (37.01.02) to a *captured biometric sample* (37.03.25) can 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.

37.02.02
biometric identification system
system that aims to perform *biometric identification* (37.08.02)

37.02.03
biometric system
system for the purpose of the *biometric recognition* (37.01.03) of individuals based on their behavioural and biological characteristics

Note 1 to entry: A biometric system will contain both *biometric* (37.01.01) and non-biometric components.

37.02.04
biometric verification system
system that aims to perform *biometric verification* (37.08.03)

IECNORM.COM : Click to view the full PDF of ISO/IEC 2382-37:2022

© ISO/IEC 2022 – All rights reserved

37.02.05
mode
DEPRECATED biometric, noun
combination of a *biometric characteristic* (37.01.02) type, a sensor type and a processing method

Note 1 to entry: The processing algorithm may contain multiple methods, details of which are not necessarily externally apparent. Thus, a *biometric system* (37.02.03) 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 will depend on convention. For example, current convention is that images of ridge patterns from both thumbs and fingers represent 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
multimodal
multiple in at least two out of three constituents of a *mode* (37.02.05) in a single *biometric system* (37.02.03)

Note 1 to entry: Multiple implies difference in type.

37.02.07
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.

Note 2 to entry: This term is used to express the extent of take-up and use of a *biometric system* (37.02.03).

37.02.08
biometric fusion
combination of *biometric* (37.01.01) information from different sources to inform a *comparison decision* (37.03.26) within a biometric *transaction* (37.06.45)

Note 1 to entry: The sources can be at the signal, feature, score, rank or decision level.

37.02.09
monobiometric system
biometric system (37.02.03) of which all of the following components are required to be singular: *biometric capture subsystem* (37.02.01), *biometric instance* (37.03.46), *biometric characteristic* (37.01.02) type, *biometric algorithm* (37.04.02) and *biometric presentation* (37.06.07)

Note 1 to entry: This term is needed for completeness. It can be the case that few systems are monobiometric, as multiple instances and multipresentations are normally allowed.

37.02.10
multibiometric system
biometric system (37.02.03) of which at least one of the following components is required to be multiple: *biometric capture subsystem* (37.02.01), *biometric instance* (37.03.46), *biometric characteristic* (37.01.02) type, *biometric algorithm* (37.04.02) or *biometric presentation* (37.06.07)

37.02.11
multipresentation system
system that accepts multiple interactions of the *biometric capture subject* (37.07.03) with the *biometric capture subsystem* (37.02.01) to obtain signals from a *biometric characteristic* (37.01.02) needed for a single *transaction* (37.06.45)

Note 1 to entry: The interaction is seen from the perspective of the biometric capture subject.

IECNORM.COM : Click to view the full PDF of ISO/IEC 2382-37:2022

37.02.12
multibiometric, adj
based on multiple types of *biometric characteristics* (37.01.02)

EXAMPLE A biometric system that is based on two or more biometric characteristic types such as two or more of face, voice, finger, iris, retina, hand geometry, signature/sign, keystroke, lip movement, gait, vein, DNA, ear, foot, scent, etc.

3.3 Terms related to data in biometric systems

37.03.01
anonymized biometric data record
biometric data record (37.03.08) purposely disassociated from individual metadata

Note 1 to entry: The *biometric data* (37.03.06) within the biometric data record ultimately remains attributable to an individual.

37.03.02
biometric application database
database of *biometric data* (37.03.06) and associated metadata developed from and supporting the operation of a *biometric* (37.01.01) application

Note 1 to entry: The metadata may include *transaction* (37.06.45) history; authorizations (e.g. age) of the *biometric data subject* (37.07.05); and archived biometric data.

Note 2 to entry: The term application includes the policies that govern the operation of the *biometric system* (37.02.03) 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* (37.01.01) process

Note 1 to entry: The application decision may include more than a *comparison* (37.05.07) process. For example, a *biometric capture process* (37.05.02) may show that there are no *biometric characteristics* (37.01.02) to capture and a decision can be made on this before any biometric characteristics are compared.

Note 2 to entry: Biometric application decisions can be made on the basis of complex policies involving both *biometric data* (37.03.06) and non-biometric data.

37.03.04
biometric candidate
biometric reference identifier (37.03.19) of a *biometric reference* (37.03.16) in the *biometric reference database* (37.03.17) determined to be sufficiently similar to the *biometric probe* (37.03.14) to warrant further analysis

Note 1 to entry: Identification systems can be configured to return a fixed number of the most similar candidates and, in other cases, the system could be configured to return candidates with *biometric candidate scores* (37.03.24) that exceed a *threshold* (37.03.36).

37.03.05
biometric candidate list
set of zero, one or more *biometric candidates* (37.03.04)

Note 1 to entry: The biometric candidate list can be tentative if it is to be reduced by further processing.

37.03.06
biometric data
biometric sample (37.03.21) or aggregation of biometric samples at any stage of processing

EXAMPLE *Biometric reference* (37.03.16), *biometric probe* (37.03.14), *biometric feature* (37.03.11) or *biometric property* (37.03.15).

IECNORM.COM : Click to view the full PDF of ISO/IEC 2382-37:2022

© ISO/IEC 2022 – All rights reserved

Note 1 to entry: 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)

37.03.08
biometric data record
data record containing *biometric data* (37.03.06)

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

37.03.09
biometric enrolment database
database of *biometric enrolment data record(s)* (37.03.10)

Note 1 to entry: A database of *biometric data* (37.03.06) not attributable to *biometric data subjects* (37.07.05) is a *biometric database* (37.03.07), but not a biometric enrolment database, e.g. data for Universal Background Models.

Note 2 to entry: The biometric enrolment database can optionally contain the *biometric reference database* (37.03.17). Separation of the databases can be required due to security, privacy, legislation, architecture, performance, etc.

Note 3 to entry: A single *biometric reference* (37.03.16) (e.g. a fingerprint on a storage card) can be considered as a biometric enrolment database in some *transactions* (37.06.45).

37.03.10
biometric enrolment data record
data record attributed to a *biometric data subject* (37.07.05), containing non-biometric data and associated with *biometric reference identifier(s)* (37.03.19)

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)* (37.03.18) or pointer(s) to biometric reference data record(s).

Note 3 to entry: The associated *biometric reference* (37.03.16) can be null (for example, *biometric enrollee* (37.07.06) lacks the *biometric characteristic* (37.01.02) or *biometric capture process* (37.05.02) is pending.

37.03.11
biometric feature
number or label extracted from *biometric samples* (37.03.21) and used for *comparison* (37.05.07)

Note 1 to entry: The set of numbers or labels are the output of a completed *biometric feature extraction* (37.05.04).

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.

Note 4 to entry: Biometric features may be extracted from an *intermediate biometric sample* (37.03.30).

Note 5 to entry: Filters applied to biometric samples are not themselves biometric features. However, the output of the filter applied to the biometric samples can be. Therefore, eigenfaces are not biometric features, for example.

37.03.12
biometric identification decision
comparison decision (37.03.26) as to whether a *biometric reference(s)* (37.03.16) of a particular *biometric data subject* (37.07.05) is in a *biometric reference database* (37.03.17)

Note 1 to entry: Return of a *biometric candidate list* (37.03.05) is not considered a biometric identification decision.

IECNORM.COM : Click to view the full PDF of ISO/IEC 2382-37:2022

Note 2 to entry: A positive *biometric identification* (37.08.02) process is inferred from the output of a *biometric reference identifier* (37.03.19).

37.03.13
biometric model
stored function generated from *biometric data* (37.03.06)

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* (37.07.05).

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* (37.05.04).

37.03.14
biometric probe
biometric query
biometric sample (37.03.21) or *biometric feature* (37.03.11) set input to an algorithm for *comparison* (37.05.07) to a *biometric reference(s)* (37.03.16)

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

Note 2 to entry: Typically, in a comparison process, incoming biometric samples serve as the subject of comparison*s* against objects stored as biometric references in a database.

37.03.15
biometric property
descriptive attributes of the *biometric data subject* (37.07.05) estimated or derived from the *biometric sample* (37.03.21) 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* (37.07.31) from face recognition would also be biometric properties.

37.03.16
biometric reference
one or more stored *biometric samples* (37.03.21), *biometric templates* (37.03.22) or *biometric models* (37.03.13) attributed to a *biometric data subject* (37.07.05) and used as the object of biometric *comparison* (37.05.07)

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 can be arbitrary. In some comparisons a biometric reference can potentially be used as the subject of the comparison with other biometric references or incoming biometric samples and input to a *biometric algorithm* (37.04.02) for comparison. 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.

IECNORM.COM : Click to view the full PDF of ISO/IEC 2382-37:2022

© ISO/IEC 2022 – All rights reserved

37.03.17
biometric reference database
database of *biometric reference data records* (37.03.18)

Note 1 to entry: The biometric reference database may be a subset of the *biometric enrolment database* (37.03.09), 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)* (37.03.16)

Note 1 to entry: There is not necessarily a one to one correspondence between biometric reference data records and *biometric data subjects* (37.07.05). For example, a single biometric data subject can have several reference data records and in some applications a single biometric reference data record can be associated with multiple enrolments of a biometric data subject.

37.03.19
biometric reference identifier
pointer to a *biometric reference data record* (37.03.18) in the *biometric reference database* (37.03.17)

37.03.20
biometric representation
biometric sample (37.03.21) or *biometric feature* (37.03.11) set

Note 1 to entry: This term is used in the ISO/IEC 19794 series and the ISO/IEC 39794 series for labelling a sub-record in a *biometric data record* (37.03.08).

37.03.21
biometric sample
analogue or digital representation of *biometric characteristics* (37.01.02) prior to *biometric feature extraction* (37.05.04)

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* (37.03.11) comparable directly to a *biometric probe* (37.03.14)

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

Note 1 to entry: A *biometric reference* (37.03.16) consisting of an image, or other *captured biometric sample* (37.03.25), in its original, enhanced or compressed form, is not a biometric template.

Note 2 to entry: The *biometric features* (37.03.11) are not considered to be a biometric template unless they are stored for reference.

37.03.23
biometric verification decision
comparison decision (37.03.26) determining the validity of a *biometric claim* (37.06.04) in a *verification transaction* (37.06.21)

37.03.24
biometric candidate score
comparison score (37.03.27) for a *biometric candidate* (37.03.04)

37.03.25
captured biometric sample
DEPRECATED raw biometric sample
biometric sample (37.03.21) resulting from a *biometric capture process* (37.05.02)

IECNORM.COM : Click to view the full PDF of ISO/IEC 2382-37:2022

37.03.26
comparison decision
determination of whether the *biometric probe(s)* (37.03.14) and *biometric reference(s)* (37.03.16) have the same *biometric* (37.01.01) source, based on a *comparison score(s)* (37.03.27), a decision policy(ies) including a *threshold* (37.03.36) and possibly other inputs

Note 1 to entry: A *match* (37.03.31) is a positive comparison decision. A *non-match* (37.03.33) is a negative comparison decision. A decision of "undetermined" may sometimes be given.

37.03.27
comparison score
DEPRECATED matching score
numerical value (or set of values) resulting from a *comparison* (37.05.07)

Note 1 to entry: A higher score does not necessarily mean more similar.

37.03.28
dissimilarity score
distance score
comparison score (37.03.27) 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.

37.03.29
fraudulent biometric enrolment data record
biometric enrolment data record (37.03.10) 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.

37.03.30
intermediate biometric sample
biometric sample (37.03.21) resulting from *intermediate biometric sample processing* (37.05.09)

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

37.03.31
match, noun
comparison decision (37.03.26) stating that the *biometric probe(s)* (37.03.14) and the *biometric reference* (37.03.16) 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* (37.05.07) 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
based on a paired *biometric probe* (37.03.14) and *biometric reference* (37.03.16) that are from the same *biometric characteristic* (37.01.02) of the same *biometric data subject* (37.07.05)

Note 1 to entry: While ‘*match*’ (37.03.31) is the result of a *comparison decision* (37.03.26), ‘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, noun
comparison decision (37.03.26) stating that the *biometric probe(s)* (37.03.14) and the *biometric reference* (37.03.16) are not from the same source

IECNORM.COM : Click to view the full PDF of ISO/IEC 2382-37:2022

37.03.34
non-mated, adj
based on a paired *biometric probe* (37.03.14) and *biometric reference* (37.03.16) that are not from the same *biometric characteristic* (37.01.02) of the same *biometric data subject* (37.07.05)

Note 1 to entry: While ‘*non-match*' (37.03.33) is the result of a *comparison decision* (37.03.26), ‘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 (37.03.27) that increases with similarity

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

37.03.37
unidentified biometric data
biometric data (37.03.06) whose *biometric data subject* (37.07.05) is currently unknown

37.03.38
conformant biometric reference rate
proportion of *biometric enrolment data records* (37.03.10) containing *biometric references* (37.03.16) *conformant* (37.06.31) with system policy

Note 1 to entry: Some *biometric systems* (37.02.03) require the enrolment of all applicants regardless of the availability of acquirable *biometric characteristics* (37.01.02). This ratio, which depends upon system capabilities and policies regulating acquisition of *biometric samples* (37.03.21), characterizes the percentage of a given enrolled population that has conformant biometric references in the biometric enrolment data records.

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

37.03.39
biometric reference rate
proportion of *biometric enrolment data records* (37.03.10) that contain a *biometric reference* (37.03.16)

Note 1 to entry: Some *biometric systems* (37.02.03) require the enrolment of all applicants regardless of the availability of acquirable *biometric characteristics* (37.01.02). This ratio, which depends upon system capabilities and policies regulating acquisition of *biometric samples* (37.03.21), characterizes the percentage of a given enrolled population that has any biometric references in the biometric enrolment data records**.**

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.

37.03.40
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.

37.03.41
reference ageing
DEPRECATED template ageing
change in error rates with respect to a fixed reference caused by time-related changes in the *biometric characteristic* (37.01.02)

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

Note 2 to entry: Reference ageing can include sample ageing, template ageing and model ageing.

IECNORM.COM : Click to view the full PDF of ISO/IEC 2382-37:2022

37.03.42
acquired biometric sample
captured biometric sample (37.03.25) assessed as suitable for subsequent *biometric feature extraction* (37.05.04) and *comparison* (37.05.07)

37.03.43
acquisition profile
list of attributes pertaining to the collection environment, the data capture subsystem, the *biometric data subject* (37.07.05), subsequent processing and management of the data

Note 1 to entry: Acquisition profiles are dependent on the modality.

37.03.44
biometric application conformance profile
listing of standards to be applied for a specific function or task

Note 1 to entry: Application *profiles* (37.03.48) *identify* (37.08.05) the use of particular options in base standards and provide a basis for conformant applications and interoperability of systems.

37.03.45
biometric data breach
unauthorized access, disclosure, alteration, transmission or processing of the *biometric data* (37.03.06) of an individual

Note 1 to entry: This definition does not apply to collection and storage even if unauthorized.

Note 2 to entry: Authorization is a jurisdictional responsibility (e.g. a government or a data subject) and limited to the purposes for which the data was collected.

37.03.46
biometric instance
occurrence of a *biometric characteristic* (37.01.02)

Note 1 to entry: A human hand typically has five instances of a fingerprint biometric characteristic.

Note 2 to entry: Multiple presentations of the same spoken or written phrase is a single instance.

37.03.47
multi-instance
requiring two or more instances of a *biometric characteristic* (37.01.02)

Note 1 to entry: The typical human hand contains more than one instance of a fingerprint biometric characteristic.

37.03.48
profile
list of attributes pertaining to an entity or a class of entities

37.03.49
pseudonymized biometric data record
biometric data record (37.03.08) purposely dis-associated from non-biometric personally identifiable information

Note 1 to entry: The *biometric data* (37.03.06) within the biometric data record ultimately remain attributable to an individual.

Note 2 to entry: This definition is consistent with the term pseudonymization in the EU General Data Protection Regulation 2016/679.

37.03.50
normalize
rescale of values for *comparison* (37.05.07) against a common or standardized scale

Note 1 to entry: Rescaling can be linear or non-linear.

IECNORM.COM : Click to view the full PDF of ISO/IEC 2382-37:2022

© ISO/IEC 2022 – All rights reserved

Note 2 to entry: The standardized scale may specify a range for the scores, a polarity or a distribution.

3.4 Terms related to devices

37.04.01
biometric capture device
device that collects a signal from a *biometric characteristic* (37.01.02) and converts it to a *captured biometric sample* (37.03.25)

Note 1 to entry: 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 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 sensors, etc.

37.04.02
biometric algorithm
set of instructions and rules for processing *biometric samples* (37.03.21)

Note 1 to entry: The complete processing of biometric signals and data may involve: signal detection, segmentation, *biometric feature extraction* (37.05.04), quality assessment, *biometric model* (37.03.13) generation, *biometric template* (37.03.22) generation, *comparison* (37.05.07), *biometric comparison decision* (37.03.26), compression, decompression, etc.

3.5 Terms related to functioning

37.05.01
biometric acquisition process
biometric capture process (37.05.02) and additional processing to attempt to produce a suitable *biometric sample(s)* (37.03.21) in accordance with the defined policy

Note 1 to entry: In addition to the biometric capture process, 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 from a single *biometric capture* (37.06.03) and each biometric sample is attributable to a single *biometric characteristic* (37.01.02). For example, four fingerprints in a slap image and 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.

37.05.02
biometric capture process
series of actions undertaken to effect a *biometric capture* (37.06.03)

EXAMPLE To obtain an International Civil Aviation Organisation (ICAO) compliant passport photograph, the *biometric capture subject* (37.07.03) 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.

Note 2 to entry: The biometric capture process may involve a single *biometric capture device* (37.04.01) or may be distributed over time and space in such a way that there is no single definable biometric capture device.

IECNORM.COM : Click to view the full PDF of ISO/IEC 2382-37:2022

37.05.03
biometric enrolment
DEPRECATED registration
act of creating and storing a *biometric enrolment data record* (37.03.10) 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* (37.01.03) in favour of enrolment.

Note 2 to entry: Enrolment in a *biometric system* (37.02.03) can in some cases not involve storage of *biometric data* (37.03.06), for example, when biometric data from an *enrollee* (37.07.06) cannot be acquired.

37.05.04
biometric feature extraction
process applied to a *biometric sample* (37.03.21) with the intent of isolating and outputting repeatable and distinctive numbers or labels which can be compared to those extracted from other biometric samples

Note 1 to entry: The creation of filters to be applied to biometric samples is not biometric feature extraction. However, the application of filters to biometric samples can 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 of the same *biometric data subject* (37.07.05).

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

Note 4 to entry: Biometric feature extraction can fail.

Note 5 to entry: Biometric feature extraction can be applied to an *intermediate biometric sample* (37.03.30).

37.05.05
biometric reference adaptation
automatic incremental updating of a *biometric reference* (37.03.16)

Note 1 to entry: Biometric reference adaptation can be used to improve performance (e.g. adapting the reference to take account of variability of an individual's *biometric characteristics* (37.01.02) and to mitigate performance degradation (e.g. due to changes in biometric characteristics over time).

37.05.06
biometric search
examination of a *biometric reference database* (37.03.17) against a *biometric probe* (37.03.14) to return either a *biometric candidate list* (37.03.05) or a *comparison decision* (37.03.26) that the biometric probe is sufficiently similar to one or more *biometric references* (37.03.16)

Note 1 to entry: Output of the biometric candidate list or the comparison decision implies implementation of a policy.

Note 2 to entry: The biometric reference database need not contain *biometric data* (37.03.06) from multiple *biometric data subjects* (37.07.05).

37.05.07
comparison
DEPRECATED match
DEPRECATED matching
estimation, calculation or measurement of similarity or dissimilarity between a *biometric probe(s)* (37.03.14) and a *biometric reference(s)* (37.03.16)

37.05.08
enrol
create and store a *biometric enrolment data record* (37.03.10) in accordance with the *biometric enrolment* (37.05.03) policy

IECNORM.COM : Click to view the full PDF of ISO/IEC 2382-37:2022

© ISO/IEC 2022 – All rights reserved

37.05.09
intermediate biometric sample processing
any manipulation of a *biometric sample* (37.03.21) that does not produce *biometric features* (37.03.11)

EXAMPLE Cropping, down-sampling, compression, conversion to data interchange formats standard and image enhancement.

Note 1 to entry: *Intermediate biometric sample* (37.03.30) processing changes the representation of the signal or data.

37.05.10
one-to-one comparison
process in which a *biometric probe(s)* (37.03.14) from one *biometric data subject* (37.07.05) is compared to a *biometric reference(s)* (37.03.16) from one biometric data subject to produce a *comparison score* (37.03.27).

Note 1 to entry: In the case of a *multimodal* (37.02.06) *biometric system* (37.02.03), the biometric probe and the biometric reference can contain multiple biometric *modes* (37.02.05).

Note 2 to entry: Some one-to-one comparison algorithms, i.e. those using score normalization, cohort models or likelihood-ratios, can require *comparisons* (37.05.07) 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
DEPRECATED one-to-few comparison
process in which *biometric probe(s)* (37.03.14) of one *biometric data subject* (37.07.05) is compared against the *biometric references* (37.03.16) of more than one biometric data subject to return a set of *comparison scores* (37.03.27)

Note 1 to entry: The term "compared" refers to *comparison* (37.05.07) in the *biometric* (37.01.01) sense.

37.05.12
one-to-many search
process in which *biometric probe(s)* (37.03.14) of one *biometric data subject* (37.07.05) is searched against the *biometric references* (37.03.16) of more than one biometric data subject to return a *biometric candidate list* (37.03.05) or a *comparison decision* (37.03.26)

Note 1 to entry: The term "searched", in the above definition, refers to *biometric search* (37.05.06).

Note 2 to entry: Output of a biometric candidate list or the comparison decision implies implementation of a policy.

37.05.13
re-enrolment
process of establishing a new *biometric reference* (37.03.16) for a *biometric data subject* (37.07.05) already *enrolled* (37.05.08) in the *biometric enrolment database* (37.03.09)

Note 1 to entry: Re-enrolment requires new *captured biometric sample(s)* (37.03.25).

37.05.14
threshold, verb
filter, verb
eliminate *biometric reference identifier(s)* (37.03.19) associated with *biometric reference(s)* (37.03.16) and/or identifiers for *biometric probe(s)* (37.03.14) that have failed to attain a level of any type of score

Note 1 to entry: Score can be *quality score* (37.09.13), *comparison score* (37.03.27), etc.

IECNORM.COM : Click to view the full PDF of ISO/IEC 2382-37:2022

3.6 Terms related to interaction

37.06.01
acceptable biometric capture attempt
capture attempt (37.06.08) that fulfils the requirements of a *biometric capture process* (37.05.02)

Note 1 to entry: 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* (37.05.01)

37.06.03
biometric capture
obtaining and recording of, in a retrievable form, signal(s) of *biometric characteristic(s)* (37.01.02) directly from individual(s), or from representation(s) of biometric characteristic(s)

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 or generated elsewhere and affected by the biometric characteristic. For example, face illuminated by incident light.

37.06.04
biometric claim
claim that a *biometric capture subject* (37.07.03) is or is not the bodily source of a specified or unspecified *biometric reference* (37.03.16)

Note 1 to entry: A biometric claim can be made by any *user* (37.07.20) of the *biometric system* (37.02.03).

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

Note 3 to entry: Claims can be positive, i.e. that the biometric capture subject is *enrolled* (37.05.08); 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* (37.07.06); or non-specific, i.e. that the biometric capture subject is or is not among the set or subset of biometric enrollees.

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

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

Note 6 to entry: The biometric claim has to fall within the biometric system boundary.

37.06.05
biometric false acceptance
error of accepting a *biometric claim* (37.06.04) that ought to have been rejected in accordance with an authoritative statement on the origin of the *biometric probe* (37.03.14) and the *biometric reference* (37.03.16)

37.06.06
biometric false rejection
error of rejecting a *biometric claim* (37.06.04) that ought to have been accepted in accordance with an authoritative statement on the origin of the *biometric probe* (37.03.14) and the *biometric reference* (37.03.16)

IECNORM.COM : Click to view the full PDF of ISO/IEC 2382-37:2022

© ISO/IEC 2022 – All rights reserved

37.06.07
biometric presentation
interaction of the *biometric capture subject* (37.07.03) and the *biometric capture subsystem* (37.02.01) to obtain a signal from a *biometric characteristic* (37.01.02)

Note 1 to entry: The biometric capture subject is not necessarily aware that a signal from a biometric characteristic is being captured.

37.06.08
capture attempt
interaction of the *biometric capture subject* (37.07.03) with the *biometric capture subsystem* (37.02.01) with the intent of producing a *captured biometric sample* (37.03.25)

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

Note 2 to entry: The "activity" taken can 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* (37.07.03) behaviours in a *capture attempt* (37.06.08)

37.06.10
capture transaction
one or more *capture attempts* (37.06.08) with the intent of acquiring all of the *biometric data* (37.03.06) from a *biometric capture subject* (37.07.03) necessary to produce either a *biometric reference* (37.03.16) or a *biometric probe* (37.03.14)

37.06.11
cognizant presentation
presentation made with the *biometric capture subject's* (37.07.03) awareness

37.06.12
conformant capture attempt
interaction by the *biometric capture subject* (37.07.03) with the *biometric capture subsystem* (37.02.01) that conforms to the *capture task* (37.06.09)

37.06.13
cooperative presentation
presentation by a *cooperative biometric capture subject* (37.07.11)

Note 1 to entry: The cooperative biometric capture subject can potentially be untrained and perform the *biometric capture task* (37.06.09) poorly or incorrectly. Therefore, a cooperative presentation can not be a *conformant capture attempt* (37.06.12).

37.06.14
negative biometric claim
assertion that a *biometric capture subject* (37.07.03) is not the source of specified or unspecified *biometric reference(s)* (37.03.16) in a *biometric reference database* (37.03.17)

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). Unspecified means there is no such non-biometric input provided.

37.06.15
non-conformant capture attempt
interaction by the *biometric capture subject* (37.07.03) with the *biometric capture subsystem* (37.02.01) that does not conform to the *capture task* (37.06.09)

IECNORM.COM : Click to view the full PDF of ISO/IEC 2382-37:2022

37.06.16
indifferent presentation

presentation in which the *biometric capture subject* (37.07.03) is unconcerned that the *biometric capture process* (37.05.02) is occurring

Note 1 to entry: 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* (37.07.03) is the source of specified or unspecified *biometric reference(s)* (37.03.16) in a *biometric reference database* (37.03.17)

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). Unspecified means there is no such non-biometric input provided.

37.06.18
unacceptable capture attempt

capture attempt (37.06.08) that does not fulfil the requirements of a *biometric capture process* (37.05.02)

Note 1 to entry: Requirements of a biometric capture process can be determined by the policy settings for the *biometric capture subsystem* (37.02.01) and the *biometric capture subject's* (37.07.03) behaviour.

37.06.19
uncooperative presentation

presentation by an *uncooperative biometric capture subject* (37.07.19)

Note 1 to entry: Uncooperative presentation can or can not be a *conformant capture attempt* (37.06.12).

Note 2 to entry: To be uncooperative, the *biometric capture subject* (37.07.03) has to be aware that *biometric data* (37.03.06) is being collected.

37.06.20
verification attempt

biometric claim (37.06.04) and *capture attempt(s)* (37.06.08) that together provide the inputs for *comparison(s)* (37.05.07)

37.06.21
verification transaction

one or more *verification attempts* (37.06.20) resulting in resolution of a *biometric claim* (37.06.04)

37.06.22
non-cognizant presentation

presentation made without the *biometric capture subject's* (37.07.03) awareness

Note 1 to entry: The biometric capture subject can or can not be subversive.

Note 2 to entry: The biometric capture subject can be aware of the general existence of *biometric systems* (37.02.03), but is unaware of the *biometric capture attempt* (37.06.08) of the system of interest.

37.06.23
capture subject training

instruction to an individual on system policy and required behaviour for submitting a *biometric sample* (37.03.21) and completing *transactions* (37.06.45)

Note 1 to entry: Instruction can be provided prior to or during the interaction of the *capture subject* (37.07.03) with the *biometric system* (37.02.03).

Note 2 to entry: Training can be through any of a variety of 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.

IECNORM.COM : Click to view the full PDF of ISO/IEC 2382-37:2022

© ISO/IEC 2022 – All rights reserved

37.06.24
capture subject habituation
degree of familiarity of a *biometric capture subject* (37.07.03) with the *biometric capture process* (37.05.02)

Note 1 to entry: A biometric capture subject with substantial familiarity with the biometric capture process is referred to as a *habituated capture subject* (37.07.24).

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

37.06.25
biometric presentation attack
presentation to the *biometric capture subsystem* (37.02.01) with the goal of interfering with the operation of the *biometric system* (37.02.03)

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

Note 2 to entry: Biometric presentation attacks can have a number of goals, e.g. impersonation or not being recognized.

Note 3 to entry: *Biometric systems* (37.02.03) can be unable to differentiate between presentations with the goal of interfering with the systems' operation and non-conformant presentations.

37.06.26
biometric capture avoidance attack
deliberate action to elude interactions with *biometric systems* (37.02.03)

Note 1 to entry: A biometric capture avoidance attack is characterized by the deliberate circumvention of the *biometric capture subsystem* (37.02.01) by the *biometric capture subject* (37.07.03) with the aim of not having a signal captured.

37.06.27
biometric distortion attack
presentation of deliberately altered *biometric characteristics* (37.01.02)

37.06.28
biometric concealment attack
deliberate act of not revealing one's own *biometric characteristics* (37.01.02) while interacting with a *biometric capture device* (37.04.01)

Note 1 to entry: No avoidance of the *biometric capture subsystem* (37.02.01) occurs in this attack.

37.06.29
biometric impostor attack
presentation of *biometric characteristics* (37.01.02) to impersonate another individual

37.06.30
cooperative
actively working in accordance with stated directions with the objective of achieving successful biometric operations

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

Note 2 to entry: Does not apply to *biometric capture subjects* (37.07.03) or *biometric presentations* (37.06.07) in covert environments.

Note 3 to entry: Determination of the quality of "cooperative" requires interpretation.

Note 4 to entry: A *cooperative biometric capture subject* (37.07.11) can be subversive, just as a *user* (37.07.20) who is not cooperative is not necessarily subversive.

IECNORM.COM : Click to view the full PDF of ISO/IEC 2382-37:2022

37.06.31
conformant
meeting required standards and policies

Note 1 to entry: Applied to *biometric presentations* (37.06.07), *biometric data* (37.03.06) and *users* (37.07.20).

37.06.32
cognizant
DEPRECATED aware
biometric capture subject's (37.07.03) knowledge of the existence of a *biometric capture process* (37.05.02)

Note 1 to entry: This term can be applied to *biometric presentations* (37.06.07) or biometric capture subjects.

37.06.33
acceptable capture attempt
capture attempt (37.06.08) that fulfils the requirements of a *biometric capture process* (37.05.02)

Note 1 to entry: Requirements of a biometric capture process can be determined by the policy settings for system and subject behaviour.

37.06.34
biometric presentation attack method
set of tools or techniques for implementing a *biometric presentation attack* (37.06.25)

EXAMPLE Replay attacks, use of artifacts and mutilation of *biometric characteristics* (37.01.02).

37.06.35
biometric system transaction
sequence of *biometric system* (37.02.03) processes that passes from initiation to completion and involves a *biometric capture subject* (37.07.03)

Note 1 to entry: The biometric capture subject can potentially not be *cognizant* (37.06.32) of the interaction with the biometric system.

Note 2 to entry: The transaction can terminate before any *capture attempt* (37.06.08).

37.06.36
***bona-fide* presentation**
biometric presentation (37.06.07) without the goal of interfering with the operation of the *biometric system* (37.02.03)

37.06.37
capture subject operational rejection
verification transaction (37.06.21) that does not allow the service requested by the *biometric capture subject* (37.07.03)

Note 1 to entry: Rejection can be due to *comparison* (37.05.07), system failure or policy reasons such as eligibility criteria, watchlists, fraudulent credentials, ergonomic factors, random referrals or can be unknown.

37.06.38
conformant biometric presentation
biometric presentation (37.06.07) that conforms with system policy

37.06.39
enrolment deactivation
termination of the operational use of *biometric data* (37.03.06) associated with a *biometric enrolment data record* (37.03.10)

Note 1 to entry: Deactivated biometric data can still be available for administrative uses.

IECNORM.COM : Click to view the full PDF of ISO/IEC 2382-37:2022

© ISO/IEC 2022 – All rights reserved

37.06.40
enrolment reactivation
reinstatement for operational use of enrolment *biometric data* (37.03.06) that has previously been in a deactivated state

37.06.41
de-enrolment
destruction of the *biometric data* (37.03.06) associated with a *biometric enrolment data record* (37.03.10)

Note 1 to entry: De-enrolment does not imply destruction of *transaction* (37.06.45) records.

Note 2 to entry: De-enrolment is always irreversible.

37.06.42
presentation attack detection
PAD
automated discrimination between *bona-fide presentations* (37.06.36) and *biometric presentation attacks* (37.06.25)

Note 1 to entry: PAD cannot infer the *biometric capture subject's* (37.07.03) intent.

37.06.43
presentation attack detection feature
number or label extracted from a *biometric sample* (37.03.21) or other data collected at the time of presentation and used to discriminate between *bona-fide presentations* (37.06.36) and *biometric presentation attacks* (37.06.25)

37.06.44
presentation attack instrument
PAI
biometric characteristic (37.01.02) or object used in a *biometric presentation attack* (37.06.25)

Note 1 to entry: The set of PAI includes artefacts but would also include lifeless biometric characteristics, (i.e. stemming from dead bodies) or altered biometric characteristics (e.g. altered fingerprints that are used in an attack).

37.06.45
transaction
provision of information dealt with as a single unit of work by a *biometric system* (37.02.03)

Note 1 to entry: The unit of work is defined by system policy.

Note 2 to entry: Provision can result in a response.

3.7 Terms related to personnel

37.07.01
biometric applicant
individual seeking to be *enrolled* (37.05.08) in a *biometric enrolment database* (37.03.09)

Note 1 to entry: The biometric applicant can or can not already be enrolled.

37.07.02
biometric attendant
agent of the *biometric system operator* (37.07.08) who directly interacts with the *biometric capture subject* (37.07.03)

EXAMPLE An immigration officer supervising a *biometric capture process* (37.05.02) and taking action on the *comparison decision* (37.03.26).

IECNORM.COM : Click to view the full PDF of ISO/IEC 2382-37:2022

© ISO/IEC 2022 – All rights reserved

37.07.03
biometric capture subject
individual who is the subject of a *biometric capture process* (37.05.02)

Note 1 to entry: 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* (37.01.02) and who does so for the purpose of resolving a *biometric claim* (37.06.04)

37.07.05
biometric data subject
individual whose individualized *biometric data* (37.03.06) is within the *biometric system* (37.02.03)

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* (37.01.03) algorithm. Examples of individuals contributing *biometric data* (37.03.06) 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 (37.07.05) whose *biometric data* (37.03.06) is held in a *biometric enrolment database* (37.03.09)

37.07.07
biometric operational personnel
individuals, other than the *biometric capture subjects* (37.07.03), who take an active role in the operation of the *biometric system* (37.02.03)

37.07.08
biometric system operator
person or organization who executes policies and procedures in the administration of a *biometric system* (37.02.03)

37.07.09
biometric system owner
person or organization with overall accountability for the acquisition, implementation and operation of the *biometric system* (37.02.03)

37.07.10
claimant
individual making a claim that can be verified biometrically

Note 1 to entry: The claimant does not need to be the *biometric data subject* (37.07.05).

37.07.11
cooperative biometric capture subject
biometric capture subject (37.07.03) motivated to achieve a successful completion of the *biometric acquisition process* (37.05.01)

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

37.07.12
biometric subversive concealer
subversive biometric capture subject (37.07.17) who attempts to avoid being matched to their own *biometric reference* (37.03.16)

IECNORM.COM : Click to view the full PDF of ISO/IEC 2382-37:2022

© ISO/IEC 2022 – All rights reserved

37.07.13
biometric impostor
subversive biometric capture subject (37.07.17) who performs a *biometric imposter attack* (37.06.29)

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.

37.07.14
indifferent biometric capture subject
biometric capture subject (37.07.03) who is unconcerned with the achievement of a successful *biometric acquisition process* (37.05.01)

Note 1 to entry: This implies the biometric capture subject is neither *cooperative* (37.06.30) nor uncooperative.

37.07.15
non-subversive biometric capture subject
biometric capture subject (37.07.03) who does not attempt to subvert the correct and intended system policy of the *biometric capture subsystem* (37.02.01)

37.07.16
non-subversive user
user (37.07.20) of a *biometric system* (37.02.03) who does not attempt to subvert the correct and intended system policy

37.07.17
subversive biometric capture subject
biometric capture subject (37.07.03) who attempts to subvert the correct and intended policy of the *biometric capture subsystem* (37.02.01)

37.07.18
subversive user
user (37.07.20) of a *biometric system* (37.02.03) 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* (37.07.03) who impersonates an *enrolled* (37.05.08) user.

37.07.19
uncooperative biometric capture subject
biometric capture subject (37.07.03) motivated to not achieve a successful *biometric acquisition process* (37.05.01)

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* (37.02.01).

37.07.20
user
DEPRECATED end user
any person or organization interacting in any way with a *biometric system* (37.02.03)

Note 1 to entry: 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* (37.03.06) is being collected should be referred to as *biometric capture subjects* (37.07.03).

37.07.21
biometric concealer
subversive biometric capture subject (37.07.17) who performs a *biometric concealment attack* (37.06.28)

IECNORM.COM : Click to view the full PDF of ISO/IEC 2382-37:2022

37.07.22
biometric avoider
subversive biometric capture subject (37.07.17) who performs a *biometric capture avoidance attack* (37.06.26)

Note 1 to entry: An avoider can bypass a *biometric system* (37.02.03) through any form of social engineering (bribery, for example).

37.07.23
biometric distorter
subversive biometric capture subject (37.07.17) who performs a *biometric distortion attack* (37.06.27)

37.07.24
habituated capture subject
biometric capture subject (37.07.03) with substantial familiarity with the *biometric capture process* (37.05.02)

37.07.25
non-habituated capture subject
biometric capture subject (37.07.03) without substantial familiarity with the *biometric capture process* (37.05.02)

37.07.26
biometric data controller
person or organization which, alone or jointly with others, determines the purposes, means and goals of the processing of *biometric data* (37.03.06)

37.07.27
biometric data processor
person or organization which *processes biometric data* (37.03.06) on behalf of the *biometric data controller* (37.07.26)

37.07.28
biometric data protection authority
body charged with protecting the rights of individuals with respect to the use of *biometric* (37.01.01) and non-biometric data in a *biometric system* (37.02.03)

37.07.29
biometric data protection officer
individual in an organization who is responsible for the development, implementation and communication of policy regarding the protection of *biometric data* (37.03.06) provided to their organization.

Note 1 to entry: Where the protection of biometric data is in doubt, the officer may undertake non-conformance investigations and recommend enforcement actions in keeping with applicable policy.

37.07.30
sex
classification as male, female or some other category based on an assessment of primary sexual characteristics or genotype or both

Note 1 to entry: Sex is generally assigned at birth by a third-party assessment.

Note 2 to entry: Primary sexual characteristics are any of the body structures directly concerned with reproduction.

37.07.31
gender
classification as male, female or another category based on social, cultural or behavioural factors

Note 1 to entry: Gender is generally determined through self-declaration or self-presentation and may change over time.

IECNORM.COM : Click to view the full PDF of ISO/IEC 2382-37:2022

© ISO/IEC 2022 – All rights reserved

Note 2 to entry: Depending on jurisdiction recognition, may or may not require assessment by a third party.

3.8 Terms related to application

37.08.01
authentication
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* (37.08.03) or *biometric identification* (37.08.02) is deprecated; the term *biometric recognition* (37.01.03) is preferred.

37.08.02
biometric identification
process of searching against a *biometric enrolment database* (37.03.09) to find and return the *biometric reference identifier(s)* (37.03.19) attributable to a single individual

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

37.08.03
biometric verification
process of confirming a *biometric claim* (37.06.04) through *comparison* (37.05.07)

Note 1 to entry: The term "verification", in the above definition refers to verifying *biometrics* (37.01.01).

Note 2 to entry: Use of the term "authentication" as a substitute for biometric verification is deprecated.

37.08.04
duplicate biometric enrolment check
biometric identification (37.08.02) check that may be performed as a part of the *biometric enrolment* (37.05.03) to ascertain the existing enrolment status of a *biometric data subject* (37.07.05)

37.08.05
identify
conduct a *biometric search* (37.05.06) against a *biometric enrolment database* (37.03.09) to find and return the *biometric reference identifier(s)* (37.03.19) attributable to a single individual

37.08.06
verify
confirm a *biometric claim* (37.06.04) through *comparisons* (37.05.07)

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

3.9 Terms related to performance

37.09.01
biometric mated comparison trial
comparison (37.05.07) of a *biometric probe* (37.03.14) and a *biometric reference* (37.03.16) from the same *biometric capture subject* (37.07.03) and the same *biometric characteristic* (37.01.02) 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 capture subject. Ultimately, the trial has nothing to do with the intention of the biometric capture subject.

IECNORM.COM : Click to view the full PDF of ISO/IEC 2382-37:2022

37.09.02
biometric non-mated comparison trial
comparison (37.05.07) of a *biometric probe* (37.03.14) and a *biometric reference* (37.03.16) from different *biometric data subjects* (37.07.05) 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 behaviour in the presence of impostors.

Note 2 to entry: A set of biometric non-mated comparison trials need not contain all possible comparisons of *biometric probes* (37.03.14) and biometric references from different biometric data subjects.

37.09.03
failure to acquire
FTA
failure to accept for subsequent *comparison* (37.05.07) the *biometric sample* (37.03.21) of the *biometric characteristic* (37.01.02) of interest output from the *biometric capture process* (37.05.02)

Note 1 to entry: *Acceptance* (37.09.18) of the output of a biometric capture process for subsequent comparison will depend on policy.

Note 2 to entry: Possible causes of failure to acquire include *failure to capture* (37.09.05), *failure to extract* (37.09.30), poor biometric sample *quality* (37.09.14), algorithmic deficiencies and biometric characteristics outside the range of the system.

37.09.04
failure-to-acquire rate
FTAR
proportion of a specified set of *biometric acquisition processes* (37.05.01) that were *failures to acquire* (37.09.03)

Note 1 to entry: The results of the biometric acquisition processes may be *biometric probes* (37.03.14) or *biometric references* (37.03.16).

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

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

37.09.05
failure to capture
FTC
failure of the *biometric capture process* (37.05.02) to produce a *captured biometric sample* (37.03.25) of the *biometric characteristic* (37.01.02) of interest

Note 1 to entry: The decision as to whether or not a *biometric sample* (37.03.21) has been captured depends on system policy. For example, one system can use a low-quality fingerprint whereas another can declare it a failure to capture.

37.09.06
failure to enrol
FTE
failure to create and store a *biometric enrolment data record* (37.03.10) for an eligible *biometric capture subject* (37.07.03) in accordance with a *biometric enrolment* (37.05.03) policy

Note 1 to entry: Not enrolling someone ineligible to *enrol* (37.05.08) is not a failure to enrol.

IECNORM.COM : Click to view the full PDF of ISO/IEC 2382-37:2022

© ISO/IEC 2022 – All rights reserved

37.09.07
failure-to-enrol rate
FTER
proportion of a specified set of *biometric enrolment* (37.05.03) *transactions* (37.06.45) that resulted in a *failure to enrol* (37.09.06)

Note 1 to entry: Basing the denominator on the number of biometric enrolment transactions can result in a higher value than basing it on the number of *biometric capture subjects* (37.07.03).

Note 2 to entry: If the FTER is to measure solely transactions that fail to complete due to *quality* (37.09.14) of the submitted *biometric data* (37.03.06), the denominator should not include transactions that fail due to non-biometric reasons (i.e. lack of eligibility due to age or citizenship).

37.09.08
false match
comparison decision (37.03.26) of a *match* (37.03.31) for a *biometric probe* (37.03.14) and a *biometric reference* (37.03.16) that are from different *biometric capture subjects* (37.07.03)

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* (37.01.02) level. Sometimes a *comparison* (37.05.07) can be made between a biometric probe and a biometric reference from different biometric characteristics of a single biometric capture subject. In some of these cases, for example, when comparing Galton ridges of different fingers of the same *biometric data subject* (37.07.05), a comparison decision of match can be considered to be an error. In other cases, for example when comparing a mispronounced pass-phrase in text-dependent speaker recognition, a comparison decision of match can be considered to be correct.

37.09.09
false match rate
FMR
proportion of the completed *biometric non-mated comparison trials* (37.09.02) that result in a *false match* (37.09.08)

Note 1 to entry: The value computed for the false match rate depends on *thresholds* (37.03.36), and other parameters of the *comparison* (37.05.07) process, and the protocol defining the biometric non-mated comparison trials.

Note 2 to entry: Comparisons between the following require proper consideration (see ISO/IEC 19795-1):

— identical twins;

— different, but related *biometric characteristics* (37.01.02) from the same individual, such as left and right-hand topography.

Note 3 to entry: “Completed” refers to the computational processes required to make a *comparison decision* (37.03.26), i.e. failures to decide are excluded.

37.09.10
false non-match
comparison decision (37.03.26) of *non-match* (37.03.33) for a *biometric probe* (37.03.14) and a *biometric reference* (37.03.16) that are from the same *biometric capture subject* (37.07.03) and of the same *biometric characteristic* (37.01.02)

Note 1 to entry: There can need to be consideration on how much non-conformance to system policy on the part of the biometric capture subject is tolerated before the biometric probe and the biometric reference are deemed to be of different biometric characteristics.

IECNORM.COM : Click to view the full PDF of ISO/IEC 2382-37:2022

37.09.11
false non-match rate
FNMR
proportion of the completed *biometric mated comparison trials* (37.09.01) that result in a *false non-match* (37.09.10)

Note 1 to entry: The value computed for the false non-match rate will depend on *thresholds* (37.03.36), and other parameters of the *comparison* (37.05.07) process, and the protocol defining the biometric mated comparison trials.

Note 2 to entry: “Completed” refers to the computational processes required to make a *comparison decision* (37.03.26), i.e. failures to decide are excluded.

37.09.12
comparison trial
single *biometric probe* (37.03.14) to *biometric reference* (37.03.16) *comparison* (37.05.07) in a test of performance

37.09.13
quality score
quantitative value of the fitness of a *biometric sample* (37.03.21) to accomplish or fulfil the *comparison decision* (37.03.26)

37.09.14
quality
degree to which a *biometric sample* (37.03.21) meets the specified requirements for its targeted application

Note 1 to entry: Quality is one aspect of *biometric utility* (37.09.16).

37.09.15
biometric character
set of attributes associated with a *biometric characteristic* (37.01.02) that cannot be controlled during the *biometric acquisition process* (37.05.01)

EXAMPLE Scars, number of minutiae, blepharoptosis (droopy eyelid).

Note 1 to entry: Character are those attributes that cannot be controlled during the biometric acquisition process.

37.09.16
biometric utility
degree to which a *biometric sample* (37.03.21) supports *biometric recognition* (37.01.03) performance

Note 1 to entry: The character of the sample source, the fidelity of the processed biometric samples and the conformance of the biometric sample presentation contribute to, or similarly detract from, the utility of the biometric sample.

Note 2 to entry: Performance measures such as *FMR* (37.09.09), *FNMR* (37.09.11), *FTER* (37.09.07) and *FTAR* (37.09.04) are an indication of biometric utility.

37.09.17
verified biometric claim
biometric claim (37.06.04) confirmed through *comparisons* (37.05.07)

Note 1 to entry: Confirmation does not determine truth, but rather indicates that a *threshold* (37.03.36) has been met.

37.09.18
acceptance
allowing of a *transaction* (37.06.45) based on a *verified biometric claim* (37.09.17) and fulfilment of the mandatory business rules

IECNORM.COM : Click to view the full PDF of ISO/IEC 2382-37:2022

37.09.19
true system acceptance
allowing of a *transaction* (37.06.45) based on a *true biometric claim* (37.09.20), a *verified biometric claim* (37.09.17) and fulfilment of the mandatory business rules

Note 1 to entry: The confirmed claim can be either positive or negative.

37.09.20
true biometric claim
biometric claim (37.06.04) known to be true through information external to the *biometric system* (37.02.03) in an authoritative statement of the origin of the *biometric probe* (37.03.14) and *biometric reference* (37.03.16)

37.09.21
true system rejection
disallowing a *transaction* (37.06.45) based on either a detected *false biometric claim* (37.09.22) or an accepted *biometric claim* (37.06.04) (whether true or false) where the business rules are not met

Note 1 to entry: The biometric claim can be either positive or negative.

37.09.22
false biometric claim
biometric claim (37.06.04) known to be false through information external to the *biometric system* (37.02.03) in an authoritative statement of the origin of the *biometric probe* (37.03.14) and *biometric reference* (37.03.16)

37.09.23
biometric fidelity
degree to which a *biometric sample* (37.03.21) is representative of a *biometric characteristic* (37.01.02) or source

Note 1 to entry: The fidelity of a biometric sample includes components attributable to environment, subject behaviour and technology.

37.09.24
biometric performance assessment
evaluation of how well a *biometric system* (37.02.03) meets functional and non-functional requirements

37.09.25
biometric reference ratio
ratio of the number of *biometric enrolment data records* (37.03.10) containing any *biometric references* (37.03.16) to all biometric enrolment data records

Note 1 to entry: This can be enumerated individually for enrolment subsystems with distinct enrolment policies.

Note 2 to entry: Non-conformant references are considered as references.

Note 3 to entry: Some *biometric systems* (37.02.03) require the enrolment of all applicants regardless of the availability of acquirable *biometric characteristics* (37.01.02). This ratio, which depends upon system capabilities and policies regulating the acquisition of *biometric samples* (37.03.21), characterizes the percentage of a given enrolled population that has any biometric references in the biometric enrolment data records.

37.09.26
capture subject operational reject rate
proportion of *verification transactions* (37.06.21) that result in an operational rejection of the *biometric capture subject* (37.07.03)

Note 1 to entry: Operational rejections are not limited to those associated with the biometric elements of the *biometric system* (37.02.03).

IECNORM.COM : Click to view the full PDF of ISO/IEC 2382-37:2022