TECHNICAL REPORT

ISO/IEC TR 29119-13

First edition

Software and systems engineering — Software testing —

Part 13: Using the ISO/IEC/IEEE 29119 series in the testing of biometric systems

PROOF/ÉPREUVE

Reference number
ISO/IEC TR 29119-13:2022(E)

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

Foreword v

Introduction vi

1 Scope 1

2 Normative references 1

3 Terms, definitions and abbreviated terms 1
3.1 Terms and definitions 1
3.2 Abbreviated terms 7

4 Introduction to biometrics 9
4.1 Biometrics overview 9
4.2 Standardization and biometrics 9
4.2.1 Introduction to standardization of biometrics 9
4.2.2 ISO/IEC JTC 1/SC 37 (biometrics) 9
4.2.3 ISO/IEC JTC 1/SC 37/WG5 (biometrics and testing) 10

5 Introduction to software testing 10
5.1 Software testing in context 10
5.2 Static and dynamic testing 10
5.3 Systematic software testing 10
5.4 Purpose of testing 11
5.5 Standardization and software testing 11
5.5.1 Testing standards prior to the ISO/IEC/IEEE 29119 series 11
5.5.2 The ISO/IEC/IEEE 29119 series 11
5.5.3 ISO/IEC JTC 1/SC 7/WG 26 (software testing) 12
5.6 Risk-based testing 12
5.6.1 Risk-based testing at the core of software testing 12
5.6.2 Risk categories 13

6 Software testing of biometric systems and subsystems 13
6.1 Traditional evaluation of biometric systems 13
6.1.1 General 13
6.1.2 Evaluation levels for biometric systems 13
6.1.3 Performance measures for biometric systems 17
6.2 Scope of testing for biometric systems 18
6.2.1 General 18
6.2.2 Biometric enrolment and recognition 18
6.2.3 Biometric components and supporting components 18
6.2.4 Biometric subsystem as part of a larger system 18
6.2.5 Static and dynamic testing of the biometric system 19
6.2.6 Testing all quality characteristics or limited to biometric performance 19
6.3 Documentation for testing biometric systems 19
6.4 Standards for testing biometric systems 19

Annex A (informative) **Brief introduction to biometric systems** 20

Annex B (informative) **Standards related to the testing of biometric systems** 26

Annex C (informative) **Generic risks in biometric systems** 32

Annex D (informative) **Test documentation mappings for biometric systems** 76

Annex E (informative) **Mapping from ISO/IEC 19795-1 to the ISO/IEC/IEEE 29119 series** 96

Annex F (informative) **Mapping from ISO/IEC 19795-2 to the ISO/IEC/IEEE 29119 series** 149

Annex G (informative) **Mapping from ISO/IEC 19795-4 to the ISO/IEC/IEEE 29119 series** 193

Annex H (informative) **Mapping from ISO/IEC 19795-6 to the ISO/IEC/IEEE 29119 series** 225

Annex I (informative) **Mapping from ISO/IEC 19795-7 to the ISO/IEC/IEEE 29119 series** 235

Annex J (informative) **Mapping from ISO/IEC TS 19795-9 to the ISO/IEC/IEEE 29119 series** 246
Annex K (informative) **Mapping from ISO/IEC 29109-1 to the ISO/IEC/IEEE 29119 series** 260
Bibliography 271

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 JTC1, *Information technology*, Subcommittee SC 7, *Software and systems engineering*.

A list of all parts in the ISO/IEC/IEEE 29119 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.

Introduction

This document provides an overview of the topics of biometric systems and software testing and their standardization. It describes how to apply the ISO/IEC/IEEE 29119 series of software testing standards to the testing of both pure biometric systems and more extensive systems that include biometric subsystems.

It includes information on the creation of a risk-based test strategy that addresses the full range of quality characteristics for a system (i.e. not restricted or focused solely on those quality characteristics covered by biometric technical performance testing).

This document includes mappings between the documentation requirements of:

— ISO/IEC 19795-1

— ISO/IEC 19795-2

— ISO/IEC 19795-6

and the software test documentation defined by ISO/IEC/IEEE 29119-3.

It provides mappings between the ISO/IEC/IEEE 29119 series and the following standards defining the testing of biometric systems:

— ISO/IEC 19795-1

— ISO/IEC 19795-2

— ISO/IEC 19795-4

— ISO/IEC 19795-6

— ISO/IEC 19795-7

— ISO/IEC TS 19795-9

— ISO/IEC 29109-1

The standards covering the evaluation and testing of biometric systems (e.g. the ISO/IEC 19795 series) are written from the perspective of an expert in biometric systems, are focused on technical biometric performance testing (i.e. error rates and throughput rates) based on dynamic testing and do not explicitly use a risk-based approach to the testing, as required by the ISO/IEC/IEEE 29119 series of software testing standards.

This document has been created to provide support to software testers who are inexperienced in testing biometric systems. It lists the most relevant biometric standards for software testers of biometric systems. It provides information on performing systematic software testing (static and dynamic) of biometric systems using a risk-based approach in conformance with the ISO/IEC/IEEE 29119 series of software testing standards. The mappings also show how conformance with the most popular biometric testing standards maps to the requirements of the ISO/IEC/IEEE 29119 series. This document also provides useful information for biometrics experts, who want to test a complete biometric system using a risk-based approach in conformance with the ISO/IEC/IEEE 29119 series of software testing standards.

As a Technical Report, this document contains data of a different kind from that normally published as an International Standard or Technical Specification, such as data on the “state of the art”.

TECHNICAL REPORT ISO/IEC TR 29119-13:2022(E)

Software and systems engineering — Software testing —

Part 13: Using the ISO/IEC/IEEE 29119 series in the testing of biometric systems

1 Scope

This document:

- gives information for software testers for the systematic, risk-based testing of biometric systems and larger systems which include biometric subsystems;
- establishes the importance of both biometric standards and software testing standards and provides overviews of both areas and their standardization;
- specifies the most important biometric standards for software testers of biometric systems;
- provides information for software testers who wish to conform to both the relevant biometrics standards and the ISO/IEC/IEEE 29119 series of software testing standards by providing mappings between the two sets of standards;
- is not limited to the testing of the technical performance of biometric systems in terms of error rates and throughput rates, but instead covers the testing of the full range of relevant quality characteristics, such as reliability, availability, maintainability, security, conformance, usability, human factors, and privacy regulation compliance;
- gives information on applying a risk-based testing approach to the testing of biometric systems that covers the full range of product and project risks;
- provides testers with an example set of product and project risks associated with biometric systems along with suggestions on how these risks can be treated as part of a risk-based approach to the testing;
- includes mappings between the documentation requirements of ISO/IEC 19795-1, ISO/IEC 19795-2 and ISO/IEC 19795-6 and the software test documentation defined by ISO/IEC/IEEE 29119-3.

2 Normative references

There are no normative references in this document.

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

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

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/

3.1.1
biometric characteristic
biological and behavioural characteristic of an individual from which distinguishing, repeatable *biometric features* (3.1.3) can be extracted for the purpose of *biometric recognition* (3.1.6)

EXAMPLE 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.

[SOURCE: ISO/IEC 2382-37:2022, 37.01.02, modified — The deprecated term has been removed.]

3.1.2
biometric data
biometric sample (3.1.9) or aggregation of biometric samples at any stage of processing

EXAMPLE *Biometric reference* (3.1.7), *biometric probe* (3.1.5), *biometric feature* (3.1.3) or biometric property.

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

[SOURCE: ISO/IEC 2382-37:2022, 37.03.06]

3.1.3
biometric feature
number or label extracted from *biometric samples* (3.1.9) and used for *comparison* (3.1.14)

[SOURCE: ISO/IEC 2382-37:2022, 37.03.11, modified — Notes to entry have been removed.]

3.1.4
biometric identification
process of searching against a biometric enrolment database to find and return the *biometric reference* (3.1.7) identifier(s) attributable to a single individual

[SOURCE: ISO/IEC 2382-37:2022, 37.08.02, modified — Note 1 to entry has been removed.]

3.1.5
biometric probe
biometric query
biometric sample (3.1.9) or *biometric feature* (3.1.3) set input to an algorithm for biometric *comparison* (3.1.14) to a *biometric reference(s)* (3.1.7)

Note 1 to entry: In some comparisons, a biometric reference can be used as the subject of the comparison with other biometric references or incoming biometric 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 comparisons against all other biometric references in the database.

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

[SOURCE: ISO/IEC 2382-37:2022, 37.03.14, modified — "biometric query" has been changed from a preferred term to an admitted term.]

3.1.6
biometric recognition
biometrics
automated recognition of individuals based on their biological and behavioural characteristics

Note 1 to entry: Biometric recognition encompasses *biometric verification* (3.1.12) and *biometric identification* (3.1.4).

Note 2 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.

[SOURCE: ISO/IEC 2382-37:2022, 37.01.03, modified — The original notes 1, 2, 5 and 6 to entry have been removed; notes 3 and 4 to entry have been renumbered as notes 1 and 2 to entry.]

3.1.7
biometric reference
one or more stored *biometric samples* (3.1.9), *biometric templates* (3.1.11) or biometric models attributed to a *biometric data* (3.1.2) subject and used as the object of biometric *comparison* (3.1.14)

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 samples and input to an biometric algorithm 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.

[SOURCE: ISO/IEC 2382-37:2022, 37.03.16]

3.1.8
biometric reference adaptation
automatic incremental updating of a *biometric reference* (3.1.7)

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* (3.1.1) and to mitigate performance degradation (e.g. due to changes in biometric characteristics over time).

[SOURCE: ISO/IEC 2382-37:2022, 37.05.05]

3.1.9
biometric sample
analogue or digital representation of *biometric characteristics* (3.1.1) prior to *biometric feature* (3.1.3) extraction

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

[SOURCE: ISO/IEC 2382-37:2022, 37.03.21]

3.1.10
biometric system
system for the purpose of the *biometric recognition* (3.1.6) of individuals based on their behavioural and biological characteristics

[SOURCE: ISO/IEC 2382-37:2022, 37.02.03, modified — Note 1 to entry has been removed.]

3.1.11
biometric template
reference biometric feature set
set of stored *biometric features* (3.1.3) comparable directly to a *biometric probe* (3.1.5)

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

Note 1 to entry: A *biometric reference* (3.1.7) consisting of an image, or other *captured biometric sample* (3.1.13), in its original, enhanced or compressed form, is not a biometric template.

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

[SOURCE: ISO/IEC 2382-37:2022, 37.03.22, modified — "reference biometric feature set" has been changed from a preferred term to an admitted term.]

3.1.12
biometric verification
DEPRECATED: authentication
process of confirming a biometric claim through *comparison* (3.1.14)

[SOURCE: ISO/IEC 2382-37:2022, 37.08.03, modified — Notes to entry have been removed; the deprecated term has been added.]

3.1.13
captured biometric sample
DEPRECATED: raw biometric sample
biometric sample (3.1.9) resulting from a biometric capture process

[SOURCE: ISO/IEC 2382-37:2022, 37.03.25]

3.1.14
comparison
DEPRECATED: match
DEPRECATED: matching
estimation, calculation or measurement of similarity or dissimilarity between *biometric probe(s)* (3.1.5) and *biometric reference(s)* (3.1.7)

[SOURCE: ISO/IEC 2382-37:2022, 37.05.07]

3.1.15
decision policy
one or more rules used to determine whether a biometric *comparison* (3.1.14) results in a positive or negative match

Note 1 to entry: The decision policy often includes a threshold above which a comparison score is considered a match.

3.1.16
detection error trade-off
DET
relationship between false-negative and false-positive errors of a binary classification system as the discrimination threshold varies

Note 1 to entry: The DET may be represented as a DET table or a DET plot.

Note 2 to entry: The receiver operating characteristic (ROC) curve was used in the previous edition of this document. The ROC is unified with the DET.

[SOURCE: ISO/IEC 19795-1:2021, 3.28]

3.1.17
failure to acquire
FTA
failure to accept for subsequent *comparison* (3.1.14) the *biometric sample* (3.1.9) of the *biometric characteristic* (3.1.1) of interest output from the biometric capture process

Note 1 to entry: Acceptance 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* (3.1.19), failure to extract, poor biometric sample quality, algorithmic deficiencies and biometric characteristics outside the range of the system.

[SOURCE: ISO/IEC 2382-37:2022, 37.09.03]

3.1.18
failure-to-acquire rate
FTAR
proportion of a specified set of biometric acquisition processes that were *failures to acquire* (3.1.17)

Note 1 to entry: The results of the biometric acquisition processes may be *biometric probes* (3.1.5) or *biometric references* (3.1.7).

Note 2 to entry: The experimenter specifies which biometric probe (or biometric reference) acquisitions are in the set, as well as the criteria for deeming 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.

[SOURCE: ISO/IEC 2382-37:2022, 37.09.04]

3.1.19
failure to capture
FTC
failure of the biometric capture process to produce a *captured biometric sample* (3.1.13) of the *biometric characteristic* (3.1.1) of interest

Note 1 to entry: The decision as to whether or not a biometric sample 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.

[SOURCE: ISO/IEC 2382-37:2022, 37.09.05]

3.1.20
failure to enrol
FTE
failure to create and store a biometric enrolment data record for an eligible biometric capture subject in accordance with a biometric enrolment policy

Note 1 to entry: Not enrolling someone ineligible to enrol is not a failure to enrol.

[SOURCE: ISO/IEC 2382-37:2022, 37.09.06]

3.1.21
failure-to-enrol rate
FTER
proportion of a specified set of biometric enrolment transactions that resulted in a *failure to enrol* (3.1.20)

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.

Note 2 to entry: If the FTER is to measure solely transactions that fail to complete due to quality of the submitted *biometric data* (3.1.2), the denominator should not include transactions that fail due to non-biometric reasons (i.e. lack of eligibility due to age or citizenship).

[SOURCE: ISO/IEC 2382-37:2022, 37.09.07]

3.1.22
false accept rate
FAR
proportion of verification transactions with false biometric claims erroneously accepted

[SOURCE: ISO/IEC 19795-1:2021, 3.21]

3.1.23
false match
comparison (3.1.14) decision of a match for a *biometric probe* (3.1.5) and a *biometric reference* (3.1.7) that are from different biometric capture subjects

Note 1 to entry: It is recognized that this definition considers the false match at the subject level only, and not at the *biometric characteristic* (3.1.1) level. Sometimes a comparison 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* (3.1.2) subject, 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.

[SOURCE: ISO/IEC 2382-37:2022, 37.09.08]

3.1.24
false match rate
FMR
proportion of the completed biometric non-mated *comparison* (3.1.14) trials that result in a *false match* (3.1.23)

Note 1 to entry: The value computed for the false match rate depends on thresholds, and other parameters of the comparison 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* (3.1.1) 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, i.e. failures to decide are excluded.

[SOURCE: ISO/IEC 2382-37:2022, 37.09.09]

3.1.25
false-negative identification rate
FNIR
FNIR(*N*, *R*, *T*)
proportion of a specified set of *identification transactions* (3.1.30) by capture subjects enrolled in the system for which the subject’s correct reference identifier is not among those returned

Note 1 to entry: The false-negative identification rate can be expressed as a function of *N*, the number of enrolees, and of parameters of the identification process where only candidates up to rank *R*, and with a candidate score greater than threshold *T* are returned to the candidate list.

[SOURCE: ISO/IEC 19795-1:2021, 3.22, modified — "FNIR(*N*, *R*, *T*)" has been changed from a preferred term to an admitted term.]

3.1.26
false non-match
comparison (3.1.14) decision of non-match for a *biometric probe* (3.1.5) and a *biometric reference* (3.1.7) that are from the same biometric capture subject and of the same *biometric characteristic* (3.1.1)

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.

[SOURCE: ISO/IEC 2382-37:2022, 37.09.10]

3.1.27
false non-match rate
FNMR
proportion of the completed biometric mated *comparison* (3.1.14) trials that result in a *false non-match* (3.1.26)

Note 1 to entry: The value computed for the false non-match rate will depend on thresholds, and other parameters of the comparison 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, i.e. failures to decide are excluded.

[SOURCE: ISO/IEC 2382-37:2022, 37.09.11]

3.1.28
false-positive identification rate
FPIR
FPIR(*N*, *T*)
proportion of *identification transactions* (3.1.30) by capture subjects not enrolled in the system, where an identifier is returned

Note 1 to entry: The false-positive identification rate can be expressed as a function of parameters of the identification process for returning matched reference identifiers including comparison score threshold (*T*), and the number of enrolees in the system (*N*).

[SOURCE: ISO/IEC 19795-1:2021, 3.23, modified — "FPIR(*N*, *T*)" has been changed from a preferred term to an admitted term; the original notes 1 and 2 to entry have been replaced by a new note 1 to entry.]

3.1.29
false reject rate
FRR
proportion of verification transactions with true biometric claims erroneously rejected

[SOURCE: ISO/IEC 19795-1:2021, 3.20]

3.1.30
identification transaction
sequence of one or more capture attempts and biometric searches to find and return the *biometric reference* (3.1.7) identifier(s) attributable to a single individual

[SOURCE: ISO/IEC 19795-1:2021, 3.10]

3.1.31
multi-modal biometric system
biometric system (3.1.10) based on multiple *biometric characteristics* (3.1.1)

3.1.32
throughput rate
number of subjects that can be processed by a *biometric system* (3.1.10) per unit time

Note 1 to entry: The throughput rate is dependent on both the system characteristics and those of the subjects.

3.2 Abbreviated terms

API	application programming interface
BIT	built-in test
BDIR	biometric data interchange record

CPU	central processing unit
CMC	cumulative match characteristic
DAC	digital-to-analogue converter
DET	detection error trade-off
EQ	equal
FAR	false accept rate
FAS	failure at source
FIF	fusion information format
FTA	failure to acquire
FTAR	failure-to-acquire rate
FTC	failure to capture
FTE	failure to enrol
FTER	failure-to-enrol rate
FMR	false match rate
FNIR	false-negative identification rate
FNMR	false non-match rate
FPIR	false-positive identification rate
FRR	false reject rate
GDPR	General Data Protection Regulation
GFAR	generalized false accept rate
GFRR	generalized false reject rate
GT	greater than
GTE	greater than or equal
HTER	half total error rate
IBDR	input biometric data record
ICAO	International Civil Aviation Organization
IEEE	Institute of Electrical and Electronics Engineers
INC	incremental
LT	less than
LTE	less than or equal
MO	member of

MRP	machine-readable passport
NEQ	not-equal
OS	operating system
RACI	responsible, accountable, consulted, and informed
RAM	random access memory
RBT	risk-based testing
ROC	receiver operating characteristic
ROM	read-only memory

4 Introduction to biometrics

4.1 Biometrics overview

Biometric systems are used to recognize people based on their physiological and/or behavioural characteristics. A key benefit is that the user does not have to carry a token of their identity (e.g. an identity card), which can be lost or stolen, or remember one or more passwords, as their identity can be recognized from their in-built traits. Example biometric characteristics used by biometric systems include, among others: fingerprints, faces, hands, retinas, and voices.

Biometric systems and biometric subsystems within larger systems are becoming more prevalent and critical to people’s daily lives. These systems are used to recognize people in a range of contexts, such as border management, voter authentication, law enforcement, and access to a variety of entities (e.g. computer systems, personal devices, and physical areas, such as buildings and entertainment events).

Annex A provides a brief introduction to biometrics for those new to the field (e.g. testers who have been asked to test their first biometric system or system including a biometric subsystem).

4.2 Standardization and biometrics

4.2.1 Introduction to standardization of biometrics

Standardization aims to promote innovation, help improve system quality, and ensure user safety, while creating a fair and open industry ecosystem. Biometric standardization occurs at various levels, including:

- international standards organizations;
- regional standards organizations;
- national standards;
- other standards organizations.

Under Joint Technical Committee 1 (JTC1) of ISO and IEC, Subcommittee 37 (ISO SC 37) is specifically responsible for biometrics standards, although biometric systems are also covered by other ISO/IEC committees and groups, such as SC 17 (Cards and security devices for personal identification) and SC 27 (Information security, cybersecurity and privacy protection).

4.2.2 ISO/IEC JTC 1/SC 37 (biometrics)

ISO/IEC JTC 1/SC 37 covers the standardization of generic biometric technologies pertaining to human beings to support interoperability and data interchange among applications and systems. Generic