International Standard

ISO/IEC 9868

Information technology — Design, development, use and maintenance of biometric identification systems involving passive capture subjects

Technologies de l'information — Conception, développement, utilisation et maintenance des systèmes d'identification biométriques appliqués sur des sujets de capture passifs

First edition
2025-02

Reference number
ISO/IEC 9868:2025(en)

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

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).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

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*.

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

Recent improvements in biometric systems, and in particular face recognition, have allowed new usage for identification systems. Biometric systems using artificial intelligence (AI) techniques are capable of capturing biometric data in publicly accessible spaces without any deliberate action from the capture subjects and possibly even without their knowledge.

On 13 March 2024, the European Commission adopted a proposal for a regulation laying down a "uniform legal framework in particular for the development, marketing and use of artificial intelligence".[1] This is one of the first-ever proposed horizontal regulations in the field of AI, aiming at building appropriate standards for safe and human-centric AI systems.

The regulation includes a risk-based framework with a tiered approach. The framework prohibits the use of certain systems posing a particularly high risk to the fundamental rights and safety of individuals, sets out requirements for high-risk AI systems and introduces transparency requirements for other AI systems. The regulation defines high-risk systems, which are systems that pose a risk of harm to the fundamental rights, health or safety of individuals. Biometric identification systems involving passive capture subjects (referred to as "remote biometric identification systems" in the words of the proposal) are classified as high-risk in the regulation risk-based framework. Providers and owners of high-risk systems are expected to demonstrate compliance with European Union (EU) regulatory requirements and identify design/operational risks and mitigation measures before they are put on the European market.

With this development in mind, this document is intended to provide international standardization in a sector which requires strong guidelines and harmonized practices in order to respond to concerns related to privacy protection, bias and accurate performance. It establishes requirements for the design, development, evaluation, operation and maintenance of biometric identification systems involving passive capture subjects.

Many of the examples and use cases found in this document focus on face and face-related biometric systems, given that face biometric characteristics are currently the more commonly used biometric characteristic. Gait and voice are other examples of usable biometric characteristics.

Information technology — Design, development, use and maintenance of biometric identification systems involving passive capture subjects

1 Scope

This document provides recommendations and requirements for the design, development, use and maintenance of biometric identification systems involving passive capture subjects, including pre- and post-deployment evaluation.

While the emphasis is on surveillance systems, this document is also applicable to other types of biometric identification systems involving passive capture subjects, regardless of biometric characteristic or sensing technology. This includes systems involving passive capture of subjects where some capture subjects enrolled voluntarily.

This document does not apply to biometric verification systems and biometric identification systems only involving capture subjects deliberately taking part in the capture.

This document does not define specific services, platforms or tools.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 2382-37, *Information technology — Vocabulary — Part 37: Biometrics*

ISO/IEC 19795-1:2021, *Information technology — Biometric performance testing and reporting — Part 1: Principles and framework*

ISO/IEC 19795-2, *Information technology — Biometric performance testing and reporting — Part 2: Testing methodologies for technology and scenario evaluation*

ISO/IEC 19795-6, *Information technology — Biometric performance testing and reporting — Part 6: Testing methodologies for operational evaluation*

ISO/IEC 19795-10, *Information technology — Biometric performance testing and reporting – Part 10: Quantifying biometric system performance variation across demographic groups*

ISO/IEC 29794-1, *Information technology — Biometric sample quality — Part 1: Framework*

ISO/IEC 30107-3, *Information technology — Biometric presentation attack detection — Part 3: Testing and reporting*

ISO/IEC 29100, *Information technology — Security techniques — Privacy framework*

ISO/IEC 24745, *Information security, cybersecurity and privacy protection — Biometric information protection*

ISO/IEC 22989, *Information technology — Artificial intelligence — Artificial intelligence concepts and terminology*

ISO/IEC 27001, *Information security, cybersecurity and privacy protection — Information security management systems — Requirements*

ISO/IEC 27002, *Information security, cybersecurity and privacy protection — Information security controls*

ISO/IEC 27005, *Information security, cybersecurity and privacy protection — Guidance on managing information security risks*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 22989 and in ISO/IEC 2382-37 and the following 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 Roles

3.1.1
biometric capture subject
individual who is the subject of a biometric capture process

Note 1 to entry: The individual remains a biometric capture subject only during the biometric capture process.

[SOURCE: ISO/IEC 2382-37:2022, 37.07.03]

3.1.2
biometric system developer
individual or organization that performs development activities (including requirements analysis, design, testing through acceptance) during the system or software life cycle process

Note 1 to entry: While the *biometric system provider* (3.1.3) and biometric system developer can be different entities, all requirements defined in this document for the biometric system developer are under the responsibility of the biometric system provider.

[SOURCE: ISO/IEC 25000:2014, 4.6, modified — Preferred term has been changed from "developer" to "biometric system developer" and Note 1 to entry has been added.]

3.1.3
biometric system provider
natural or legal person, public authority, agency or other body that places a *biometric identification system involving passive capture subjects (BISPCS)* (3.2.1) on the market or puts it into service under its own name or trademark, whether for payment or free of charge

3.1.4
biometric system owner
person or organization with overall accountability for the acquisition, implementation and operation of the biometric system

Note 1 to entry: The biometric system owner is known as the "user" in the EU AI Act.[1]

[SOURCE: ISO/IEC 2382-37:2022, 37.07.09, modified — Note 1 to entry has been added.]

3.1.5
experimenter
individual responsible for defining, designing and analysing the test

[SOURCE: ISO/IEC 19795-1:2021, 3.5]

3.1.6
biometric system operator
person or organization who executes policies and procedures in the administration of a biometric system

Note 1 to entry: In the context of this document, the biometric system operator designates staff from the *biometric system owner* (3.1.4) operating the system

[SOURCE: ISO/IEC 2382-37:2022, 37.07.08, modified — Note 1 to entry has been added.]

3.1.7
passive capture subject
individual who is the subject of a biometric capture process where biometric data capture does not require any deliberate action of biometric presentation by the *biometric capture subject* (3.1.1)

Note 1 to entry: Passive capture subjects are often unaware that their biometric data is being captured and unable to prevent capture.

3.1.8
test crew member
selected biometric data subject whose use of the operational system is controlled or monitored as part of the evaluation

Note 1 to entry: In an operational evaluation, test subjects can be subjects of the operational system or they can be members of a test crew using the system specifically for evaluation purposes.

[SOURCE: ISO/IEC 19795-6:2012, 4.17]

3.2 Categories of biometric identification system and use cases

3.2.1
biometric identification system involving passive capture subjects
BISPCS
biometric identification system where biometric data capture does not require any deliberate action of biometric presentation by the *biometric capture subject* (3.1.1)

EXAMPLE 1 A biometric identification system capturing *passive capture subjects* (3.1.7) walking in a designated area to create biometric probes is a BISPCS.

EXAMPLE 2 A biometric system where biometric capture subjects actively and knowingly participate in the biometric data capture process is not a BISPCS.

EXAMPLE 3 An access control system to a secured building where the personnel have voluntarily enrolled in the biometric reference database is not a BISPCS.

Note 1 to entry: A BISPCS can implement *watchlist identification* (3.2.2).

3.2.2
watchlist identification
process of searching a probe from a *biometric capture subject* (3.1.1) against a biometric reference database to return biometric reference identifier(s) attributable to a biometric person of interest

EXAMPLE A biometric system searching for a missing child in a publicly accessible space.

Note 1 to entry: In watchlist identification scenarios, most biometric capture subjects are not mated to references in the watchlist. Therefore, the expected result is that no reference is returned.

3.2.3
video surveillance system
VSS
system consisting of camera equipment, monitoring and associated equipment for transmission and controlling purposes, which can be necessary for the surveillance of a protected area

[SOURCE: ISO/IEC 30137-1:2024, 3.2.12]

3.3 Miscellaneous

3.3.1
demographic group
category of the human population, defined by specific traits or criteria

EXAMPLE Ethnic group, gender, age group, but also people having facial hair/not having facial hair, wearing make-up/not wearing make-up, wearing accessories/not wearing accessories, etc.

Note 1 to entry: The recognition performance of a biometric identification system can vary across different demographic groups.

3.3.2
manual review
human intervention to achieve a biometric decision

Note 1 to entry: Human intervention can encompass all aspects of a biometric system policy.

3.3.3
monitoring mechanism
mechanism which enables the *biometric system owner* (3.1.4) to assess whether or not the system is functioning as expected

4 Abbreviated terms

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

AI	artificial intelligence
ATM	automated teller machine
BISPCS	biometric identification systems involving passive capture subjects
CAPNIR	concealer attack presentation non-identification rate
CMC	cumulative match characteristic (as defined in ISO/IEC 19795-1)
FND	false negative differential
FNIR	false negative identification rate
FPD	false positive differential
FPIR	false positive identification rate
FRT	face recognition technology
FTAR	failure-to-acquire rate
FTER	failure-to-enrol rate
ML	machine learning
PAD	presentation attack detection
VIP	very important person
VSS	video surveillance system

5 Conformance

Requirements of this document can apply to multiple stakeholders. Some requirements are the responsibility of the biometric system provider. Some requirements are the responsibility of the biometric system owner. Some requirements are the responsibility of both the biometric system provider and biometric system owner. A BISPCS is conformant with this document only if the biometric system provider and the biometric system owner fulfil all their responsibilities.

The biometric system developer can be different from the biometric system provider, but all requirements assigned to the developer are under the responsibility of the biometric system provider.

The biometric system provider, in coordination with the biometric system developer where appropriate, shall document the following:

- the system's intended purpose;
- the rationale for development of the biometric algorithm to process captured data to achieve its intended purpose;
- operating assumptions and limitations;
- types of biometric characteristic to be captured and processed;
- quality and compatibility requirements;
- biometric performance characteristics;
- BISPCS use cases;
- how fitness for purpose for BISPCS use cases is determined.

The biometric system provider can be the same as the biometric system owner, such as a government agency with the resources and skill to train new models using custom internal algorithms.

Biometric system providers and biometric system owners shall fulfil all the responsibilities summarized in Table 1.

Table 1 — Roles and responsibilities

Topic		Role	Representative responsibilities	Applicable Clause/subclause
Risk assessment		Biometric system provider	Assessment for intended use case of the system and provision of suitable mitigation measures	Clause 7
		Biometric system owner	Document assessment for the intended use case	
Design and development		Biometric system provider	Appropriate development of the BISPCS, and testing and validation of all required technical functionalities	Clauses 8 and 9
Operational practice	Competence of biometric system operators	Biometric system provider	Provide training	10.2
		Biometric system owner	Ensure competence is validated	
	Operational security	Biometric system owner	Ensure that the system utilizes appropriately configured and maintained security controls	10.3