

AS ISO/IEC 24741:2024  
ISO/IEC 24741:2024



STANDARDS  
Australia



# Information technology — Biometrics — Overview and application

Currently in preview, click buy full version

AS ISO/IEC 24741:2024

This Australian Standard® was prepared by IT-032, Biometrics and Identification. It was approved on behalf of Standards Australia's Standards Development and Accreditation Committee on 20 November 2024.

This Standard was published on 6 December 2024.

The following are represented on Committee IT-032:

- Department of Defence (Australian Government)
- Department of Foreign Affairs and Trade (DFAT)
- Department of Home Affairs — Digital and Technology Policy Division
- Photo Marketing Association
- SITA

This Standard was issued in draft form for comment as DR AS ISO/IEC 24741:2024.

#### **Keeping Standards up-to-date**

Ensure you have the latest versions of our publications and keep up-to-date about Amendments, Rulings, Withdrawals, and new projects by visiting:

[www.standards.org.au](http://www.standards.org.au)

ISBN 978 1 76139 953 4

# Information technology — Biometrics — Overview and application

First published as AS ISO/IEC 24741:2024.

## **COPYRIGHT**

© ISO/IEC 2024 — All rights reserved  
© Standards Australia Limited 2024

All rights are reserved. No part of this work may be reproduced or copied in any form or by any means, electronic or mechanical, including photocopying, without the written permission of the publisher, unless otherwise permitted under the Copyright Act 1968 (Cth).

## Preface

This Standard was prepared by the Standards Australia Committee IT-032, Biometrics and Identification.

The objective of this document is to describe the history and purpose of biometrics, the various biometric technologies in general use today (for example, fingerprint recognition, face recognition and iris recognition) and the architecture of the systems and the system processes that allow automated recognition using those technologies. It provides information on the application of biometrics in various business domains, such as border management, law enforcement and driver licensing. It also provides information on the societal and jurisdictional considerations that are typically taken into account in biometric systems.

Additionally, this document provides guidance on the use of the Standards that underpin the use of biometric recognition systems.

This document is identical with, and has been reproduced from, ISO/IEC 24741:2024, *Information technology — Biometrics — Overview and application*.

As this document has been reproduced from an international document, a full point substitutes for a comma when referring to a decimal marker.

Australian or Australian/New Zealand Standards that are identical adaptations of international normative references may be used interchangeably. Refer to the online catalogue for information on specific Standards.

The terms “normative” and “informative” are used in Standards to define the application of the appendices or annexes to which they apply. A “normative” appendix or annex is an integral part of a Standard, whereas an “informative” appendix or annex is only for information and guidance.

# Contents

Preface .....	ii
Foreword .....	v
Introduction .....	vi
<b>1 Scope .....</b>	<b>1</b>
<b>2 Normative references .....</b>	<b>1</b>
<b>3 Terms, definitions and abbreviated terms .....</b>	<b>1</b>
3.1 Terms and definitions .....	1
3.2 Abbreviated terms .....	1
<b>4 Fundamentals of biometrics .....</b>	<b>2</b>
4.1 Biometric characteristics .....	2
4.2 Biometric systems .....	3
<b>5 History .....</b>	<b>5</b>
<b>6 Overview of biometric technologies .....</b>	<b>6</b>
6.1 Finger and palm ridge recognition .....	6
6.1.1 Fingerprint imaging .....	6
6.1.2 Fingerprint comparison .....	7
6.1.3 Palm technologies .....	8
6.2 Face recognition .....	8
6.3 Iris recognition .....	9
6.4 Dynamic signature recognition .....	10
6.5 Vascular recognition .....	10
6.6 Hand geometry recognition .....	10
6.7 Voice recognition .....	11
6.8 DNA recognition .....	11
6.9 Full body recognition .....	11
6.10 Gait recognition .....	12
6.11 Retina recognition .....	12
6.12 Keystroke recognition .....	12
6.13 Scent and odour recognition .....	12
6.14 Cardiogram recognition .....	12
6.15 Multimodal biometrics .....	12
<b>7 General biometric systems .....</b>	<b>13</b>
7.1 Conceptual representation of general biometric system .....	13
7.2 Conceptual components of a general biometric system .....	13
7.2.1 Data capture .....	13
7.2.2 Transmission .....	14
7.2.3 Signal processing .....	14
7.2.4 Data storage .....	14
7.2.5 Comparison .....	14
7.2.6 Decision .....	15
7.2.7 Administration .....	15
7.2.8 Interface to external application .....	15
7.3 Functions of general biometric system .....	16
7.3.1 Enrolment .....	16
7.3.2 Verification of a positive biometric claim .....	16
7.3.3 Identification .....	17
<b>8 Example applications .....</b>	<b>18</b>
8.1 General .....	18
8.2 Physical access control .....	18
8.3 Logical access control .....	18
8.4 Time and attendance .....	19

8.5	Accountability.....	19
8.6	Electronic authorizations.....	19
8.7	Government and citizen services.....	19
8.8	Border protection.....	19
8.8.1	ePassports and machine-readable travel documents.....	19
8.8.2	Automated border control (ABC) systems.....	20
8.8.3	Entry/exit systems.....	20
8.8.4	Visas.....	20
8.8.5	EURODAC.....	20
8.9	Law enforcement.....	20
8.10	Civil background checks.....	21
8.11	Clustering.....	21
<b>9</b>	<b>Performance testing.....</b>	<b>21</b>
9.1	General.....	21
9.2	Types of technical tests.....	22
<b>10</b>	<b>Biometric technical interfaces.....</b>	<b>23</b>
10.1	Biometric data blocks (BDBs) and biometric information record (BIRs).....	23
10.2	Management of information on source of biometric data.....	24
10.3	Service architectures.....	24
10.4	The BioAPI application programming interface.....	25
10.5	The BioAPI interworking protocol (BIP).....	25
<b>11</b>	<b>Biometrics and information security.....</b>	<b>26</b>
11.1	General.....	26
11.2	Security of biometric data.....	26
11.3	Presentation attack (spoofing) detection.....	29
11.4	Integrity of the enrolment process.....	29
<b>12</b>	<b>Biometrics and privacy.....</b>	<b>30</b>
12.1	General.....	30
12.2	Privacy protections for biometric applications.....	31
12.3	Proportional application of biometric.....	32
12.4	Biometric technology acceptability.....	32
12.5	Confidentiality of biometric data.....	32
12.6	Integrity of biometric data.....	33
12.7	Irreversibility of biometric data.....	33
12.8	Unlinkability of biometric information.....	33
<b>13</b>	<b>Overview of biometric standardisation.....</b>	<b>34</b>
13.1	Standards development organizations.....	34
13.2	Types of biometric standards.....	34
13.2.1	Biometric data interchange format standards.....	34
13.2.2	Biometric technical interface standards.....	35
13.2.3	Biometric conformance testing standards.....	36
13.2.4	Biometric sample quality standards.....	37
13.2.5	Biometric application profile standards.....	37
13.2.6	Biometric performance testing and reporting standards.....	38
13.2.7	Biometric security standards.....	38
13.2.8	Biometric authentication standards.....	39
13.2.9	Standards on cross-jurisdictional and societal aspects of biometrics.....	40
13.2.10	Biometric vocabulary standards.....	40
13.3	Criteria for selecting a standard.....	41
	<b>Bibliography.....</b>	<b>43</b>

## 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](http://www.iso.org/directives) or [www.iec.ch/members\\_experts/refdocs](http://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](http://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](http://www.iso.org/iso/foreword.html). In the IEC, see [www.iec.ch/understanding-standards](http://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 TR 24741:2018), which has been technically revised.

The main change is as follows:

- Guidance is given on the international standards that underpin the use of biometric recognition systems.

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](http://www.iso.org/members.html) and [www.iec.ch/national-committees](http://www.iec.ch/national-committees).

## Introduction

“Biometric recognition” is the automated recognition of individuals based on their biological and behavioural characteristics. The field is a subset of the broader field of human identification science. Example technologies include, among others: fingerprint recognition, face recognition, hand geometry recognition, speaker recognition and iris recognition.

Some techniques (such as iris recognition) are more biologically based, whereas some (such as signature recognition) are more behaviourally based, but all techniques are influenced by both behavioural and biological elements. There are no purely “behavioural” or “biological” biometric systems.

“Biometric recognition” is frequently referred to as simply “biometrics”, although the term “biometrics” has also historically been associated with the statistical analysis of general biological data. The word “biometrics”, like “genetics”, is usually treated as singular. It first appeared in the vocabulary of physical and information security around 1980 as a substitute for the earlier descriptor “automatic personal identification” in use in the 1970s. Biometric systems recognize “persons” by recognizing “bodies”. The distinction between person and body is subtle but is of key importance in understanding the inherent capabilities and limitations of these technologies. Within the context of JTC 1/SC 37 documents, biometrics deals with computer-based recognition of patterns created by human behaviours and biological structures and is usually associated more with the field of computer engineering and statistical pattern analysis than with the behavioural or biological science.

Today, biometrics is used to recognize individuals in a wide variety of contexts, such as computer and physical access control, law enforcement, voting, border control, social benefit programs and driver licencing.

# Australian Standard®

## Information technology — Biometrics — Overview and application

### 1 Scope

This document describes the history and purpose of biometrics, the various biometric technologies in general use today (for example, fingerprint recognition, face recognition and iris recognition) and the architecture of the systems and the system processes that allow automated recognition using those technologies. It provides information on the application of biometrics in various business domains such as border management, law enforcement and driver licencing. It also provides information on the societal and jurisdictional considerations that are typically taken into account in biometric systems.

Additionally, this document provides guidance on the use of the International Standards that underpin the use of biometric recognition systems.

### 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*

### 3 Terms, definitions and abbreviated terms

#### 3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 2382-37 apply.

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

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

#### 3.2 Abbreviated terms

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

ABC	automated border control
API	application programming interface
AFIS	automated fingerprint identification system
AFIS	automated biometric identification system
LB	biometric data block
BIAS	biometric identity assurance services
BIR	biometric information record
BIP	Biometric Interworking Protocol
CBEFF	Common Biometric Exchange Formats Framework
CNN	convolutional neural network