INTERNATIONAL STANDARD

**ISO/IEC 24745**

Second edition
2022-02

# Information security, cybersecurity and privacy protection — Biometric information protection

*Securité de l'information, cybersécurité et protection de la vie privée — Protection des informations biométriques*

Reference number
ISO/IEC 24745:2022(E)

© ISO/IEC 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



© ISO/IEC 2022 – All rights reserved

# Contents

Page

**Foreword** ..... **v**
**Introduction** ..... **vi**
**1 Scope** ..... **1**
**2 Normative references** ..... **1**
**3 Terms and definitions** ..... **1**
**4 Abbreviated terms** ..... **6**
**5 Biometric systems** ..... **7**
5.1 General ..... 7
5.2 Biometric system operations ..... 9
5.3 Biometric references and identity references (IRs) ..... 11
5.4 Biometric systems and identity management systems ..... 11
5.5 Personally identifiable information (PII) and privacy ..... 12
5.6 Societal considerations ..... 12
**6 Security aspects of a biometric system** ..... **13**
6.1 Security requirements for biometric systems to protect biometric information ..... 13
6.1.1 Confidentiality ..... 13
6.1.2 Integrity ..... 13
6.1.3 Renewability and revocability ..... 13
6.1.4 Availability ..... 14
6.2 Security threats and countermeasures in biometric systems ..... 14
6.2.1 Threats and countermeasures against biometric system components ..... 14
6.2.2 Threats and countermeasures during the transmission of biometric information ..... 16
6.2.3 Renewable biometric references as countermeasure technology ..... 17
6.3 Security of data records containing biometric information ..... 19
6.3.1 Security for biometric information processing in a single database ..... 19
6.3.2 Security for biometric information processing in separated databases ..... 21
**7 Biometric information privacy management** ..... **22**
7.1 Biometric information privacy threats ..... 22
7.2 Biometric information privacy requirements and guidelines ..... 22
7.2.1 Irreversibility ..... 22
7.2.2 Unlinkability ..... 23
7.2.3 Confidentiality ..... 23
7.3 Biometric information lifecycle privacy management ..... 23
7.3.1 Collection ..... 23
7.3.2 Transfer (disclosure of information to a third party) ..... 24
7.3.3 Use ..... 24
7.3.4 Storage ..... 24
7.3.5 Retention ..... 25
7.3.6 Archiving and data backup ..... 25
7.3.7 Disposal ..... 25
7.4 Responsibilities of a biometric system owner ..... 25
**8 Biometric system application models and security** ..... **26**
8.1 Biometric system application models ..... 26
8.2 Security in each biometric application model ..... 27
8.2.1 General ..... 27
8.2.2 Model A — Store on server and compare on server ..... 28
8.2.3 Model B — Store on token and compare on server ..... 29
8.2.4 Model C — Store on server and compare on client ..... 31
8.2.5 Model D — Store on client and compare on client ..... 32
8.2.6 Model E — Store on token and compare on client ..... 34

© ISO/IEC 2022 – All rights reserved

8.2.7 Model F — Store on token and compare on token ..... 36
8.2.8 Model G — Store distributed on token and server, compare on server ..... 37
8.2.9 Model H — Store distributed on token and client, compare on client ..... 38
8.2.10 Model I — Store on server, compare distributed ..... 40
8.2.11 Model J — Store on token, compare distributed ..... 41
8.2.12 Model K — Store distributed, compare distributed ..... 43

**Annex A** (informative) **Secure binding and use of separated $DB_{IR}$ and $DB_{BR}$** ..... **45**

**Annex B** (informative) **Framework for renewable biometric references (RBRs)** ..... **48**

**Annex C** (informative) **Technology examples for biometric information protection** ..... **52**

**Annex D** (informative) **Biometric watermarking** ..... **54**

**Annex E** (informative) **Biometric information protection using information splitting** ..... **56**

**Annex F** (informative) **Selection of biometric application models** ..... **58**

**Bibliography** ..... **61**


© ISO/IEC 2022 – All rights reserved

# 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 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 27, *Information security, cybersecurity and privacy protection*.

This second edition cancels and replaces the first edition (ISO/IEC 24745:2011), which has been technically revised.

The main changes compared to the previous edition are as follows:

— correction of terms;

— removal of non-compliant requirements related to jurisdictions;

— clarification of various explanations;

— improvements on the requirements for protection of biometric information, with more explicit enforcement of irreversibility and unlinkability;

— addition of relevant references to ISO/IEC 30136:2018;

— introduction of new application models based on recent technologies;

— addition of examples in annexes.

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.

© ISO/IEC 2022 – All rights reserved

# Introduction

As the Internet becomes a more pervasive part of daily life, various services are being provided via the Internet, e.g. Internet banking, remote healthcare. In order to provide these services in a secure manner, the need for authentication mechanisms between subjects and the service being provided becomes even more critical. Some of the authentication mechanisms already developed include token-based schemes, personal identification and transaction numbers (PIN/TAN), digital signature schemes based on public key cryptosystems, and authentication schemes using biometric techniques.

Biometrics, the automated recognition of individuals based on their behavioural and physiological characteristics, includes recognition technologies based on, e.g. fingerprint image, voice patterns, iris image and facial image. The cost of biometric techniques has been decreasing while their reliability has been increasing, and both are now acceptable and viable for use as an authentication mechanism.

Biometric authentication introduces a potential discrepancy between privacy and authentication assurance. On the one hand, biometric characteristics are ideally an unchanging property associated with and distinct to an individual. This binding of the credential to the individual provides strong assurance of authentication. On the other hand, this strong binding also underlies the privacy concerns surrounding the use of biometrics, such as unlawful processing of biometric data, and poses challenges to the security of biometric systems to prevent or to be resilient to the compromise of biometric references (BRs). The usual solution to the compromise of an authentication credential (to change the password or issue a new token) is not generally available for biometric authentication because biometric characteristics, being either intrinsic physiological properties or behavioural traits of individuals, are difficult or impossible to change. At most, another finger or eye instance can be enrolled, but the choices are usually limited. Therefore, appropriate countermeasures to safeguard the security of a biometric system and the privacy of biometric data subjects are essential.

Biometric systems usually bind a BR with other personally identifiable information (PII) for authenticating individuals. In this case, the binding is needed to assure the security of the data record containing biometric information. The increasing linkage of BRs with other PII and the sharing of biometric information across legal jurisdictions make it extremely difficult for organizations to assure the protection of biometric information and to achieve compliance with various privacy regulations.


© ISO/IEC 2022 – All rights reserved

# Information security, cybersecurity and privacy protection — Biometric information protection

## 1 Scope

This document covers the protection of biometric information under various requirements for confidentiality, integrity and renewability/revocability during storage and transfer. It also provides requirements and recommendations for the secure and privacy-compliant management and processing of biometric information.

This document specifies the following:

— analysis of the threats to and countermeasures inherent to biometrics and biometric system application models;

— security requirements for securely binding between a biometric reference (BR) and an identity reference (IR);

— biometric system application models with different scenarios for the storage and comparison of BRs;

— guidance on the protection of an individual's privacy during the processing of biometric information.

This document does not include general management issues related to physical security, environmental security and key management for cryptographic techniques.

## 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 30136, *Information technology — Performance testing of biometric template protection schemes*

## 3 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**
**authentication**
provision of assurance in the *identity* (3.22) of an individual

[SOURCE: ISO/IEC 29115:2013, 3.2, modified — "entity" replaced by "individual".]

© ISO/IEC 2022 – All rights reserved

**3.2**
**auxiliary data**
**AD**
subject-dependent data that are part of a *renewable biometric reference* (3.34) and may be required to reconstruct *pseudonymous identifiers* (3.29) during verification, or for verification in general

Note 1 to entry: If *auxiliary data* are part of a *renewable biometric reference*, it is not necessarily stored in the same place as the corresponding *pseudonymous identifiers*.

Note 2 to entry: *Auxiliary data* may contain data elements for *diversification* (3.19).

Note 3 to entry: *Auxiliary data* are not the element for comparison during biometric reference verification.

Note 4 to entry: *Auxiliary data* are generated by the *biometric system* (3.13) during enrolment.

EXAMPLE Secret number combined with biometric data using, for example, a helper data approach, fuzzy commitment scheme or fuzzy vault. See Table C.1 for concrete examples of *pseudonymous identifier* (PI) (3.29) and AD.

**3.3**
**biometric authentication**
*authentication* (3.1) where *biometric verification* (3.16) or *biometric identification* (3.8) is applied and the *identity* (3.22) is linked to the *biometric reference* (3.11)

**3.4**
**biometric characteristic**
biological and behavioural characteristic of an individual from which distinguishing, repeatable *biometric features* (3.7) can be extracted for the purpose of biometric recognition

[SOURCE: ISO/IEC 2382-37:2017, 3.1.2, modified — The EXAMPLE was removed.]

**3.5**
**biometric data**
*biometric sample* (3.12) or aggregation of biometric samples at any stage of processing, e.g. *biometric reference* (3.11), biometric probe, *biometric feature* (3.7) or biometric property

Note 1 to entry: As defined in ISO/IEC 2382-37:2017, 3.3.15, biometric property is a descriptive attribute of the *biometric data* (3.5) subject estimated or derived from the *biometric sample* (3.12) by automated means.

[SOURCE: ISO/IEC 2382-37:2017, 3.3.6, modified — Note 1 to entry was removed and replaced by a new Note 1 to entry.]

**3.6**
**biometric data subject**
**subject**
individual whose individualized *biometric data* (3.5) is within the *biometric system* (3.13)

[SOURCE: ISO/IEC 2382-37:2017, 3.7.5, modified — Note 1 to entry was removed.]

**3.7**
**biometric feature**
numbers or labels extracted from *biometric samples* (3.12) and used for comparison

[SOURCE: ISO/IEC 2382-37:2017, 3.3.11, modified — Notes 1 to 5 to entry were removed.]

**3.8**
**biometric identification**
process of searching against a biometric enrolment database to find and return the *biometric reference* (3.11) *identifier(s)* (3.21) attributable to a single individual

[SOURCE: ISO/IEC 2382-37:2017, 3.8.2, modified — Note 1 to entry was removed.]


© ISO/IEC 2022 – All rights reserved

**3.9**
**biometric information**
information conveyed or represented by *biometric data* (3.5)

Note 1 to entry: Biometric data include for instance data derived or transformed from biometric data which are handled in connection with biometric data within a *biometric system* (3.13).

**3.10**
**biometric model**
stored function generated from *biometric data* (3.5)

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

[SOURCE: ISO/IEC 2382-37:2017, 3.3.13, modified — Notes 1 to 3 to entry were removed.]

**3.11**
**biometric reference**
**BR**
one or more stored *biometric samples* (3.12), *biometric templates* (3.14) or *biometric models* (3.10) attributed to a *biometric data subject* (3.6) and used as the object of biometric comparison

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

Note 1 to entry: A *biometric reference* that can be renewed is referred to as a *renewable biometric reference* (3.34).

Note 2 to entry: BR can be used as a factor in multi-factor authentication, that is, something a person is.

[SOURCE: ISO/IEC 2382-37:2017, 3.3.16, modified — Notes 1 and 2 to entry were removed and replaced by new Notes 1 and 2 to entry.]

**3.12**
**biometric sample**
analog or digital representation of *biometric characteristics* (3.4) prior to *biometric feature* (3.7) extraction

[SOURCE: ISO/IEC 2382-37:2017, 3.3.21, modified — The EXAMPLE was removed.]

**3.13**
**biometric system**
system for the purpose of the biometric recognition of individuals based on their behavioural and biological characteristics

[SOURCE: ISO/IEC 2382-37:2017, 3.2.3, modified — Note 1 to entry was removed.]

**3.14**
**biometric template**
set of stored *biometric features* (3.7) comparable directly to probe biometric features

[SOURCE: ISO/IEC 2382-37:2017, 3.3.22, modified — The EXAMPLE and Notes 1 and 2 to entry were removed.]

**3.15**
**biometric template protection**
protection of *biometric references* (3.11) under various requirements for secrecy, *irreversibility* (3.26), and *renewability* (3.33) during storage and transfer

Note 1 to entry: A *biometric template protection* scheme is one example of *biometric information* (3.9) protection scheme.

[SOURCE: ISO/IEC 30136:2018, 3.3, modified — Added Note 1 to entry.]

© ISO/IEC 2022 – All rights reserved

**3.16**
**biometric verification**
process of confirming a biometric *claim* (3.17) through biometric comparison

[SOURCE: ISO/IEC 2382-37:2017, 3.8.3, modified — Note 1 to entry was removed.]

**3.17**
**claim**
assertion of *identity* (3.22)

**3.18**
**common identifier**
**CI**
*identifier* (3.21) for correlating *identity references* (3.24) and *biometric references* (3.11) in physically or logically separated databases

**3.19**
**diversification**
deliberate creation of multiple, unlinkable, transformed *biometric references* (3.11) from one or more *biometric samples* (3.12) obtained from one subject for the purposes of security and privacy enhancement

Note 1 to entry: *Renewability* (3.33) is provided by performing *diversification* for *biometric reference*(s).

**3.20**
**generative biometric data**
*biometric data* (3.5) (sample(s) or features) used as primary input to the *biometric template protection* (3.15) scheme

[SOURCE: ISO/IEC 30136:2018, 3.4]

**3.21**
**identifier**
one or more attributes that uniquely characterize an individual in a specific domain

EXAMPLE The name of a club with a club-membership number, a health insurance card number together with the name of the insurance company, an IP address, and a universal unique identifier.

**3.22**
**identity**
set of properties or characteristics of an individual that can be used to describe its state, appearance or other qualities

**3.23**
**identity management system**
**IdMS**
system controlling individual identity information throughout the information lifecycle in one domain

**3.24**
**identity reference**
**IR**
non-biometric attribute that is an *identifier* (3.21) with a value that remains the same for the duration of the existence of the individual in a domain

**3.25**
**IR claimant**
**identity reference claimant**
individual making an *identity reference* (3.24) *claim* (3.17)

Note 1 to entry: *Claims* can be verified in a number of ways, some of which may be based on biometrics.


© ISO/IEC 2022 – All rights reserved

**3.26**
**irreversibility**
property of a transform that creates a *biometric reference* (3.11) from *generative biometric data* (3.20) such that knowledge of the transformed biometric reference cannot be used to determine any information about the generative biometric data

[SOURCE: ISO/IEC 30136:2018, 3.5, modified — Note 1 to entry was removed.]

**3.27**
**personally identifiable information**
**PII**
any information that a) can be used to identify the PII principal to whom such information relates, or b) is or might be directly or indirectly linked to a PII principal

[SOURCE: ISO/IEC 29100:2011, 2.9, modified — Note 1 to entry was removed.]

**3.28**
**privacy compromise**
event in which an adversary discovers part of the *generative biometric data* (3.20) of an individual enrolled in the database of a *biometric verification* (3.16) or identification system

[SOURCE: ISO/IEC 30136:2018, 3.6, modified — Note 1 to entry was removed.]

**3.29**
**pseudonymous identifier**
**PI**
part of a *renewable biometric reference* (3.34) that represents an individual or data subject within a domain by means of a protected *identity* (3.22) that can be verified by means of a captured *biometric sample* (3.12) and the *auxiliary data* (3.2) (if any)

Note 1 to entry: A *pseudonymous identifier* should not contain any information that allows retrieval of the original *biometric sample*, the original *biometric features* (3.7), or the true identity of its owner.

Note 2 to entry: The *pseudonymous identifier* has no meaning outside the service domain.

Note 3 to entry: Encrypted *biometric data* (3.5) with a cipher that allows retrieval of the plain-text data before comparison is not a *pseudonymous identifier*.

Note 4 to entry: A *pseudonymous identifier* may be the element for comparison during *biometric reference* verification.

Note 5 to entry: See Table C.1 for examples of PI and *auxiliary data* (AD) (3.2).

**3.30**
**pseudonymous identifier comparator**
**PIC**
system, process or algorithm that compares the *pseudonymous identifier* (3.29) generated during enrolment by the *pseudonymous identifier encoder* (3.31) and the *pseudonymous identifier* reconstructed during verification by the *pseudonymous identifier recoder* (3.32), and returns a similarity score representing the similarity between the two

[SOURCE: ISO/IEC 30136:2018, 3.8]

**3.31**
**pseudonymous identifier encoder**
**PIE**
system, process or algorithm that generates a *renewable biometric reference* (3.34) consisting of a *pseudonymous identifier* (3.29) and possibly *auxiliary data* (3.2) based on a *biometric reference*

© ISO/IEC 2022 – All rights reserved

**3.32**
**pseudonymous identifier recoder**
**PIR**
system, process or algorithm that reconstructs a *pseudonymous identifier* (3.29) based on the provided *auxiliary data* (3.2) and the extracted features

[SOURCE: ISO/IEC 30136:2018, 3.9]

**3.33**
**renewability**
property of a transform or process to create multiple, unlinkable transformed *biometric references* (3.11) derived from one or more *biometric samples* (3.12) obtained from the same data subject and which can be used to recognize the individual while not revealing information about the original reference

**3.34**
**renewable biometric reference**
**RBR**
renewable *identifier* (3.21) that represents an individual or data subject within a domain by means of a protected binary *identity* (3.22) (re)constructed from the captured *biometric sample* (3.12), and fulfilling *irreversibility* (3.26) requirements

Note 1 to entry: A *renewable biometric reference* fulfilling *irreversibility* requirement provides additional security property.

Note 2 to entry: An example of a *renewable biometric reference* is a *pseudonymous identifier* (3.29) and additional data elements required for *biometric verification* (3.16) or identification such as *auxiliary data* (3.2).

**3.35**
**revocability**
ability to prevent future successful verification of a specific *biometric reference* (3.11) and the corresponding *identity reference* (3.24)

Note 1 to entry: Rejection of a subject may occur on the grounds of its appearance on a revocation list.

**3.36**
**secure channel**
communication channel providing the confidentiality and authenticity of exchanged messages

**3.37**
**token**
physical device storing *biometric reference* (3.11) and in some cases performing on-board biometric comparison

EXAMPLE Smart card, USB memory stick or RFID chip in e-passport.

**3.38**
**unlinkability**
property of two or more *biometric references* (3.11) that they cannot be linked to each other or to the subject(s) from whom they were derived

## 4 Abbreviated terms

AD auxiliary data

AFIS automated fingerprint identification systems

BR biometric reference

CI common identifier


© ISO/IEC 2022 – All rights reserved