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

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



This document is a preview generated by EUS



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

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

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

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.

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.

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".]