

---

---

**Financial services — Biometrics —  
Security framework**

*Services financiers — Biométrie — Cadre de sécurité*



This document is a preview generated by EUS



**COPYRIGHT PROTECTED DOCUMENT**

© ISO 2023

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](mailto:copyright@iso.org)  
Website: [www.iso.org](http://www.iso.org)

Published in Switzerland

# Contents

Page

<b>Foreword</b>	<b>vi</b>
<b>Introduction</b>	<b>vii</b>
<b>1 Scope</b>	<b>1</b>
<b>2 Normative references</b>	<b>1</b>
<b>3 Terms and definitions</b>	<b>2</b>
<b>4 Abbreviated terms</b>	<b>8</b>
<b>5 Biometrics in financial service context</b>	<b>8</b>
5.1 General	8
5.2 Generic security considerations	10
5.3 Personal device vulnerabilities and controls strategy	10
5.4 Biometric verification versus biometric identification	10
<b>6 Biometric modalities and core systems</b>	<b>11</b>
6.1 General	11
6.2 Modalities of biometrics	11
6.2.1 General	11
6.2.2 Fingerprint	11
6.2.3 Voice biometrics	12
6.2.4 Iris biometrics	12
6.2.5 Face biometrics	12
6.2.6 Signature biometrics	13
6.2.7 Vein biometrics	13
6.2.8 Palm print biometrics	14
6.2.9 Keystroke biometrics	14
6.3 Biometric system and its supporting systems	14
6.3.1 Overview	14
6.3.2 Core systems	15
6.3.3 Core biometric authentication usage scenarios	16
<b>7 Financial biometric authentication systems — usability considerations</b>	<b>20</b>
7.1 General	20
7.2 Properties of biometric modalities	20
7.3 Properties and evaluation of biometric system	21
7.3.1 Recognition performance	21
7.3.2 Recognition performance evaluation	22
7.3.3 Presentation attack detection	23
7.3.4 Interoperability	23
<b>8 Financial biometric authentication systems – architectures</b>	<b>24</b>
8.1 Overview	24
8.2 Conceptual business architecture	24
8.3 Technical architecture	25
8.4 Registration architecture	25
8.5 PBP devices and associated biometric authentication architectures	26
8.5.1 PBP device operators	26
8.5.2 PBP device types	28
8.5.3 Point of biometric presentation (PBP)	28
8.5.4 Biometric authentication architecture	30
<b>9 Financial biometric authentication systems – threats and vulnerabilities</b>	<b>34</b>
9.1 Generic threat considerations	34
9.2 Biometric presentation vulnerabilities	35
9.2.1 Overview	35
9.2.2 Synthetic biometric presentation attack vulnerabilities	35
9.2.3 Improper PBP device calibration vulnerabilities	36

9.2.4	Fault injection .....	36
9.3	Comparison, decision and storage subsystem vulnerabilities .....	36
9.3.1	Overview .....	36
9.3.2	Improper threshold settings vulnerability .....	37
9.3.3	Score and threshold vulnerabilities .....	37
9.3.4	Reference refinement vulnerabilities .....	37
9.3.5	Self-targeted match search vulnerabilities .....	38
9.3.6	Other-party targeted match search vulnerabilities .....	38
9.3.7	Match collision vulnerabilities .....	38
9.3.8	Authentication result transmission vulnerabilities .....	38
9.3.9	Biometric storage vulnerabilities .....	38
<b>10</b>	<b>Financial biometric authentication systems — security requirements .....</b>	<b>38</b>
10.1	General .....	38
10.2	Generic security requirements .....	38
10.2.1	Physical security requirements .....	38
10.2.2	Logical security requirements .....	39
10.3	Identity registration .....	40
10.3.1	Overview .....	40
10.3.2	Security requirements .....	40
10.4	Presentation .....	40
10.4.1	Overview .....	40
10.4.2	Security requirements .....	40
10.5	Data storage and handling .....	40
10.5.1	Overview .....	40
10.5.2	Reference splitting procedure .....	40
10.6	Comparison and decision .....	42
10.6.1	Overview .....	42
10.6.2	Security requirements .....	42
10.7	Enrolment .....	42
10.7.1	Overview .....	42
10.7.2	Security requirements .....	42
10.8	Re-enrolment .....	43
10.8.1	Overview .....	43
10.8.2	Security requirements .....	43
10.9	Refinement .....	43
10.9.1	Overview .....	43
10.9.2	Security requirements .....	43
10.10	Verification .....	43
10.10.1	Overview .....	43
10.10.2	Security requirements .....	44
10.11	Identification .....	44
10.11.1	Overview .....	44
10.11.2	Security requirements .....	44
10.12	Termination .....	45
10.12.1	Overview .....	45
10.12.2	Security requirements .....	45
10.13	Suspension and reactivation .....	45
10.13.1	Overview .....	45
10.13.2	Security requirements .....	45
10.14	Archiving .....	46
10.14.1	Overview .....	46
10.14.2	Security requirements .....	46
10.15	Security compliance verification .....	46
	<b>Annex A (informative) Threats and vulnerabilities for biometric environments .....</b>	<b>47</b>
	<b>Annex B (informative) Biometric implementation scenarios .....</b>	<b>50</b>
	<b>Annex C (normative) Biometric security controls checklist .....</b>	<b>59</b>

<b>Bibliography</b> .....	<b>64</b>
---------------------------	-----------

This document is a preview generated by EVS

## Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

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 ISO documents 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)).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO 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](http://www.iso.org/patents)).

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).

This document was prepared by Technical Committee ISO/TC 68, *Financial services*, Subcommittee SC 2, *Financial Services, security*.

This second edition cancels and replaces the first edition (ISO 19092:2008), which has been technically revised.

The main changes are as follows:

- technical developments since the first edition reflected;
- newer use cases fitting current use of biometrics in the financial industry and related security considerations included;
- built on a newer set of ISO standards for biometrics, created by ISO/IEC JTC 1/SC 37.

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).

## Introduction

Retail transaction authentication using card- and PIN-based technologies has historically been central to the protection of retail electronic transactions. However, the advent of new technologies and the evolution of old technologies has introduced the possibility of using personal biometrics as an alternative or supplementary method of transaction authentication.

Biometrics as a mechanism for recognizing individuals includes the use of fingerprints and iris and facial images.

The wide use of a biometric system with the public depends on a number of factors:

- convenience and ease of use;
- level of appropriate security;
- performance;
- non-invasiveness.

This document provides security guidelines for the integration of biometrics into the retail payment sector using card or other technologies in the financial industry from component to system level and includes recommendations regarding compliance verification. Nonetheless, the guidelines set out in this document do not guarantee that a particular implementation will be secure against all threats. It is the responsibility of the financial institutions deploying such technology, via their security risk management processes, to ensure adequate controls are in place to mitigate threats in accordance with institutional policy.





# Financial services — Biometrics — Security framework

## 1 Scope

This document specifies the security framework for using biometrics for authentication of customers in financial services, focusing exclusively on retail payments. It introduces the most common types of biometric technologies and addresses issues concerning their application. This document also describes representative architectures for the implementation of biometric authentication and associated minimum control objectives.

The following are within the scope of this document:

- use of biometrics for the purpose of:
  - verification of a claimed identity;
  - identification of an individual;
- biometric authentication threats, vulnerabilities and controls;
- validation of credentials presented at enrolment to support authentication;
- management of biometric information across its life cycle, comprising enrolment, transmission and storage, verification, identification and termination processes;
- security requirements for hardware used in conjunction with biometric capture and biometric data processing;
- biometric authentication architectures and associated security requirements.

The following are not within the scope of this document:

- detailed specifications for data collection, feature extraction and comparison of biometric data and the biometric decision-making process;
- use of biometric technology for non-financial transaction applications, such as physical or logical system access control.

## 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 9796 (all parts), *Information technology — Security techniques — Digital signature schemes giving message recovery*

ISO/IEC 9797 (all parts), *Information technology — Security techniques — Message Authentication Codes (MACs)*

ISO 11568, *Financial services — Key management (retail)*

ISO 13491-1, *Financial services — Secure cryptographic devices (retail) — Part 1: Concepts, requirements and evaluation methods*

ISO 13491-2, *Financial services — Secure cryptographic devices (retail) — Part 2: Security compliance checklists for devices used in financial transactions*

ISO/IEC 15408-3, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 3: Security assurance components*

ISO/IEC 14888 (all parts), *IT Security techniques — Digital signatures with appendix*

ISO/IEC 18033 (all parts), *Information security — Encryption algorithms*

ISO/IEC 19772, *Information security — Authenticated encryption*

### 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 biometric authentication

authentication where biometric verification or biometric identification is applied and the identity is linked to the biometric reference

[SOURCE: ISO/IEC 24745:2022, 3.3]

#### 3.2 biometric capture

obtaining and recording of, in a retrievable form, signal(s) of biometric characteristic(s) directly from individual(s), or from representation(s) of biometric characteristic(s)

[SOURCE: ISO/IEC 2382-37:2022, 37.06.03, modified — Notes to entry removed.]

#### 3.3 biometric capture device

device that collects a signal from a biometric characteristic and converts it to a captured biometric sample

[SOURCE: ISO/IEC 2382-37:2022, 37.04.01, modified — Notes to entry removed.]

#### 3.4 biometric data

biometric sample or aggregation of biometric samples at any stage of processing

[SOURCE: ISO/IEC 2382-37:2022, 37.03.06, modified — Notes to entry and example removed.]

#### 3.5 biometric enrolment

act of creating and storing a biometric enrolment data record in accordance with an enrolment policy

[SOURCE: ISO/IEC 2382-37:2022, 37.05.03, modified — Notes to entry removed.]

#### 3.6 biometric enrolment database

database of biometric enrolment data record(s)

[SOURCE: ISO/IEC 2382-37:2022, 37.03.09, modified — Notes to entry removed.]