INTERNATIONAL STANDARD

ISO 19092

Second edition
2023-03

Financial services — Biometrics — Security framework

Services financiers — Biométrie — Cadre de sécurité

Reference number
ISO 19092:2023(E)

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) 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).

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).

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.

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.

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.]

3.7
biometric feature extraction
process applied to a biometric sample with the intent of isolating and outputting repeatable and distinctive numbers or labels which can be compared to those extracted from other biometric samples

[SOURCE: ISO/IEC 2382-37:2022, 37.05.04, modified — Notes to entry removed.]

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

[SOURCE: ISO/IEC 2382-37:2022, 37.08.02, modified — Note to entry removed.]

3.9
biometric information
information conveyed or represented by biometric data

[SOURCE: ISO/IEC 24745:2022, 3.9, modified — Note to entry removed.]

3.10
biometric policy
set of rules that indicate the applicability of a biometric reference to some community or class of application having common security requirements

3.11
biometric presentation
interaction of the biometric capture subject and the biometric capture subsystem to obtain a signal from a biometric characteristic

[SOURCE: ISO/IEC 2382-37:2022, 37.06.07, modified — Note to entry removed.]

3.12
biometric reference
one or more stored biometric samples, biometric templates or biometric models attributed to a biometric data subject and used as the object of biometric comparison

[SOURCE: ISO/IEC 2382-37:2022, 37.03.16, modified — Notes to entry and example removed.]

3.13
biometric reference adaptation
automatic incremental updating of a biometric reference

[SOURCE: ISO/IEC 2382-37:2022, 37.05.05, modified — Notes to entry removed.]

3.14
biometric sample
analogue or digital representation of biometric characteristics prior to biometric feature extraction

[SOURCE: ISO/IEC 2382-37:2022, 37.03.21, modified — Example removed.]

3.15
biometric system
system for the purpose of the biometric recognition of individuals based on their behavioural and biological characteristics

[SOURCE: ISO/IEC 2382-37:2022, 37.02.03, modified — Notes to entry removed.]

3.16
biometric system-on-card
card-sized device including biometric acquisition, data processing, storage, comparison and decision to compose a complete biometric verification system

[SOURCE: ISO/IEC 24787:2018, 3.8]

3.17
biometric verification
process of confirming a biometric claim through comparison

[SOURCE: ISO/IEC 2382-37:2022, 37.08.03, modified — Notes to entry removed.]

3.18
biometrics
automated recognition of individuals based on their biological and behavioural characteristics

[SOURCE: ISO/IEC 2382-37:2022, 37.01.03, modified — Notes to entry removed.]

3.19
claimant
individual making a claim that can be authenticated in biometric authentication

[SOURCE: ISO/IEC 2382-37:2022, 37.07.10, modified — Note to entry removed and definition revised.]

3.20
comparison
estimation, calculation or measurement of similarity or dissimilarity between biometric probe(s) and biometric reference(s)

[SOURCE: ISO/IEC 2382-37:2022, 37.05.07]

3.21
comparison score
score
numerical value (or set of values) resulting from a comparison

[SOURCE: ISO/IEC 2382-37:2022, 37.03.27, modified — Note to entry removed.]

3.22
confidentiality
property that information is not available or disclosed to unauthorized individuals, entities or processes

[SOURCE: ISO/IEC 27000:2018, 3.10]

3.23
credential
representation of an identity for use in authentication

Note 1 to entry: Customary embodiments of a credential are very diverse. To accommodate this wide range, the definition adopted is very generic.

Note 2 to entry: A credential is typically made to facilitate data authentication of the identity information pertaining to the identity it represents. Data authentication is typically used in authorization.

Note 3 to entry: The identity information represented by a credential can, for example, be printed on human-readable media, or stored within a physical token. Typically, such information can be presented in a manner designed to reinforce its perceived validity.

EXAMPLE Username, username with a password, PIN, smart card, token, fingerprint, passport.

[SOURCE: ISO/IEC 24760-1:2019, 3.3.5, modified — Note 4 to entry changed to examples.]

3.24
decision policy
principles according to which a biometric system provides comparison decisions, inclusive of the following elements:

- the threshold of biometric comparison;
- the number of attempts for enrolment, verification or identification permitted per transaction;
- the number of biometric references enrolled per claimant;
- the number of distinct biometric samples (e.g. different fingerprints) enrolled per claimant;
- the number of biometric modalities (e.g. fingerprint, voice) in which the claimant is enrolled;
- other internal controls in the comparison process.

Note 1 to entry: Serial, parallel, weighted or fusion decision models in biometric systems utilize more than one biometric reference in the comparison process for a given user (e.g. using biometric references from multiple fingerprints).

3.25
encryption
(reversible) transformation of data by an encryption algorithm to produce ciphertext, i.e. to hide the information content of the data

[SOURCE: ISO/IEC 18033-1:2021, 3.11]

3.26
false match rate
FMR
proportion of the completed biometric non-mated comparison trials that result in a false match

Note 1 to entry: The value computed for the FMR will depend on thresholds, other parameters of the comparison process and the protocol defining the biometric non-mated comparison trials.

Note 2 to entry: Comparisons between:

- identical twins;
- different but related biometric characteristics from the same individual, such as left- and right-hand topography will need proper consideration (see ISO/IEC 19795-1).

Note 3 to entry: “completed” refers to the computational processes required to make a comparison decision, i.e. failures to decide are excluded.

Note 4 to entry: “non-mated” refers to cases when the compared biometrics come from different individuals.

[SOURCE: ISO/IEC 2382-37:2022, 37.09.09, modified — Note 4 to entry added.]

3.27
false-negative identification rate
FNIR
FNIR (*N*, *R*, *T*)
proportion of a specified set of identification transactions by capture subjects enrolled in the system for which the subject’s correct reference identifier is not among those returned

Note 1 to entry: The false-negative identification rate can be expressed as a function of N, the number of enrolees, and of parameters of the identification process where only candidates up to rank R and with a candidate score greater than threshold T are returned to the candidate list.

[SOURCE: ISO/IEC 19795-1:2021, 3.22]

3.28
false non-match rate
FNMR
proportion of the completed biometric matched comparison trials that result in a false non-match

[SOURCE: ISO/IEC 2382-37:2022, 37.09.11, modified — Notes to entry removed.]

3.29
false-positive identification rate
FPIR
FPIR (*N*, *T*)
proportion of identification transactions by capture subjects not enrolled in the system for which a reference identifier is returned

Note 1 to entry: The false-positive identification rate can be expressed as a function of *N*, the number of enrolees, and of parameters of the identification process where only candidates with a candidate score greater than threshold *T* are returned to the candidate list.

Note 2 to entry: For systems that always return a fixed number of candidates without applying a threshold on scores, FPIR is not a meaningful metric.

[SOURCE: ISO/IEC 19795-1:2021, 3.23]

3.30
initial enrolment
(biometric) enrolment that occurs after previous authentication of the subject, such as via a password

Note 1 to entry: See also *biometric enrolment* (3.5) and *re-enrolment* (3.38).

3.31
integrated circuit card
card containing integrated circuits and interfaces, especially used for payment or similar

3.32
integrity
property of accuracy and completeness

[SOURCE: ISO/IEC 27000:2018, 3.36]

3.33
on-card biometric comparison
comparison and decision-making on an integrated circuit card where the biometric reference is retained on-card in order to enhance security and privacy

[SOURCE: ISO/IEC 24787:2018, 3.12]

3.34
payment token
value linked to and acting as a substitute for a primary account number

3.35
point of biometric presentation
PBP
human interface device to which an account holder presents biometric characteristics, typically in conjunction with a payment card, for the purposes of carrying out a financial transaction or for enrolling their credentials for future use in such a transaction

3.36
presentation attack
presentation to the biometric data capture subsystem with the goal of interfering with the operation of the biometric system

Note 1 to entry: Presentation attack can be implemented through a number of methods, e.g. artefact, mutilations, replay.

Note 2 to entry: Presentation attacks may have a number of goals, e.g. impersonation or not being recognized.

Note 3 to entry: Biometric systems may not be able to differentiate between biometric presentation attacks with the goal of interfering with the systems operation and non-conformant presentations.

[SOURCE: ISO/IEC 30107-1:2016, 3.5]

3.37
presentation attack detection
automated determination of a presentation attack

Note 1 to entry: Presentation attack detection cannot infer the subject’s intent. In fact, it could be impossible to derive that difference from the data capture process or acquired sample

[SOURCE: ISO/IEC 30107-1:2016, 3.6]

3.38
re-enrolment
process of establishing a new biometric reference replacing existing biometric data for a subject already enrolled

Note 1 to entry: Re-enrolment requires new captured biometric sample(s).

Note 2 to entry: See also *biometric enrolment* (3.5) and *initial enrolment* (3.30).

[SOURCE: ISO/IEC 2382-37:2022, 37.05.13, modified — Definition revised and Note 2 to entry added.]

3.39
registration
process before enrolment in which a person is provided an electronic identifier and credential(s) with which he or she proves his or her identity for enrolment

Note 1 to entry: This is performed in conjunction with enrolment, such that it appears to be a single process.

3.40
secure biometric reader
SBR
secure cryptographic device embodying biometric capture device and associated biometric processing software

3.41
secure cryptographic device
SCD
device that provides physically and logically protected cryptographic services and storage (e.g. PIN entry device or hardware security module), and which can be integrated into a larger system, such as an automated teller machine (ATM) or point of sale (POS) terminal

[SOURCE: ISO 13491-1:2016, 3.28, modified — Definition revised.]

3.42
secure element
significantly tamper-resistant component providing secure storage, secure processing and confidentiality