DRAFT INTERNATIONAL STANDARD

ISO/DIS 19092

ISO/TC **68**/SC **2**

Secretariat: **BSI**

Voting begins on:
2022-04-29

Voting terminates on:
2022-07-22

Financial services — Biometrics — Security framework

Services financiers — Biométrie — Cadre de sécurité

ICS: 35.240.40; 03.060

This document is circulated as received from the committee secretariat.

Reference number
ISO/DIS 19092:2022(E)

COPYRIGHT PROTECTED DOCUMENT

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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

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.

ISO 19092 was prepared by Technical Committee ISO/TC 68, Financial services, Subcommittee SC 2, Security management and general banking operations.

The second edition of ISO 19092 replaces ISO 19092:2008. Biometrics, and biometrics as used in payments in particular, has undergone tremendous development since 2008 when the previous revision of this document was published. The current revision takes this development into account, describing newer use cases fitting today's use of biometrics and the security considerations associated. It also builds on a newer set of ISO standards for biometrics, created by ISO/IEC SC 37. Thus, the current revision substantially revises and/or replaces most parts of the previous revision.

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 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, 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 seeks to provide security guidelines for the integration of biometrics into the retail payments sector using card or other technologies in the financial industry from component to system level, and including making recommendations regarding compliance evaluation. Nonetheless, the guidelines set out into 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 accord with institutional policy.

This document replaces ISO 19092-1:2006. When ISO 19092-1:2006 was published, it was expected that a second part of ISO 19092 (ISO 19092-2, *Financial services — Biometrics — Part 2: Message syntax and cryptographic requirements*) would subsequently be published. However, ISO 19092-2 was not completed due to a lack of consensus. As a result, ISO 19092-1:2006 has been updated into this document, removing all references to ISO 19092-2 and incorporating some significant new text.

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:

— usage of biometrics for 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 physical 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:

— privacy and legal requirements; however, if any of the requirements contained in this document conflict with country, state, or local laws, the country, state, or local law will apply.

— detailed specifications for data collection, feature extraction and comparison of biometric data, and the biometric decision-making process;

— usage of biometric technology for non-financial transaction applications such as physical or logical system access control.

2 Normative references

The following referenced documents are indispensable for the application 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, *Information technology — Security techniques — Digital signature schemes giving message recovery*

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

ISO 11568, *Banking — Key management (retail)*

ISO 13491, *Financial services — Secure cryptographic devices (retail)*

ISO/IEC 14888, *IT Security techniques — Digital signatures with appendix*

ISO/IEC 18033, *Information security — Encryption algorithms*

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

ISO/IEC 19790, *Information technology — Security techniques — Security requirements for cryptographic modules*

ISO/IEC 24745, *Information security, cybersecurity and privacy protection — Biometric information protection*

ISO/IEC 30107, *Information technology — Biometric presentation attack detection*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

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, 3.3]

3.2
biometric capture
obtain and record, 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 2382-37:2017, 3.6.3]

3.3
biometric capture device
device that collects a signal from a biometric characteristic and converts it to a captured biometric sample

Note 1 to entry: A signal can be generated by the biometric characteristic or generated elsewhere and affected by the biometric characteristic, for example, face illuminated by incident light.

Note 2 to entry: A biometric capture device can be any piece of hardware (and supporting software and firmware).

Note 3 to entry: A biometric capture device may comprise components such as an illumination source, one or more biometric sensors, etc.

[SOURCE: ISO/IEC 2382-37:2017, 3.4.1]

3.4
biometric data
biometric sample or aggregation of biometric samples at any stage of processing, e.g. biometric reference, biometric probe, biometric feature or biometric property

[SOURCE: ISO/IEC 2382-37:2017, 3.3.6]

3.5
biometric enrolment
act of creating and storing a biometric enrolment data record in accordance with an enrolment policy

Note 1 to entry: Registration has a different meaning in the signal processing community and its use is therefore deprecated in biometrics in favour of enrolment.

Note 2 to entry: Enrolment in a biometric system might, in some cases, not involve storage of biometric data, for example, when biometric data from an enrolee cannot be acquired.

Note 3 to entry: This term is also used as “enrolment” in this document.

Note 4 to entry: See also *initial enrolment* (3.31) and *re-enrolment* (3.39).

[SOURCE: ISO/IEC 2382-37:2017, 3.5.3]

3.6
biometric enrolment database
database of biometric enrolment data records

[SOURCE: ISO/IEC 2382-37:2017, 3.3.9]

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 2382-37:2017, 3.5.4]

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 2382-37:2017, 3.8.2]

3.9
biometric information
information conveyed or represented by biometric data

[SOURCE: ISO/IEC 24745, 3.9]

3.10
biometric policy
named 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

Note 1 to entry: The biometric capture subject may not be aware that a signal from a biometric characteristic is being captured.

[SOURCE: ISO/IEC 2382-37:2017, 3.6.7]

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 2382-37:2017, 3.3.16]

3.13
biometric reference adaptation
automatic incremental updating of a biometric reference

[SOURCE: ISO/IEC 2382-37:2017, 3.5.5]

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

[SOURCE: ISO/IEC 2382-37:2017, 3.3.21]

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

[SOURCE: ISO/IEC 2382-37:2017, 3.2.3]

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, 3.8]

3.17
biometric verification
process of confirming a biometric claim through biometric comparison

Note 1 to entry: Use of the term "authentication" as a substitute for biometric verification is deprecated.

[SOURCE: ISO/IEC 2382-37:2017, 3.8.3]

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

[SOURCE: ISO/IEC 2382-37:2017, 3.1.3]

3.19
claimant
individual making a claim that can be verified biometrically

[SOURCE: ISO/IEC 2382-37:2017, 3.7.10]

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

[SOURCE: ISO/IEC 2382-37:2017, 3.5.7]

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

Note 1 to entry: Higher does not necessarily mean more similar.

[SOURCE: ISO/IEC 2382-37:2017, 3.3.27]

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.

Note 4 to entry: A credential can be a username, username with a password, a PIN, a smartcard, a token, a fingerprint, a passport, etc.

[SOURCE: ISO/IEC 24760-1:2019, 3.3.5]

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/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 plain text (readable) by a cryptographic algorithm to produce cipher text (unreadable) to hide the information content of the plain text

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, and 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.

[SOURCE: ISO/IEC 2382-37:2017, 3.9.9]

Note 4 to entry: "non-mated" refers to the case where the compared biometrics come from different individuals.

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, 3.22]

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

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

Note 2 to entry: "Completed" refers to the computational processes required to make a comparison decision, i.e. failures to decide are excluded.

[SOURCE: ISO/IEC 2382-37:2017, 3.9.11]

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, 3.23]

3.30
impostor
person who submits a biometric sample in either an intentional or inadvertent attempt to be authenticated as another person who is an enrolee

3.31
initial enrolment
(biometric) enrolment for the first time after another means of authentication of the biometric data subject, such as password authentication in order to confirm the identity

Note 1 to entry: See also *biometric enrolment* (3.5) and *re-enrolment* (3.39).

3.32
integrated circuit card
ICC
card containing integrated circuits and interfaces, especially used for payment or similar use

3.33
integrity
property of accuracy and completeness

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

3.34
on-card biometric comparison
comparison and decision making on an ICC where the biometric reference is retained on-card in order to enhance security and privacy

[SOURCE: ISO/IEC 24787, 3.12]

3.35
payment token
a value linked to and acting as a substitute for a PAN

3.36
point of biometric presentation
PBP
human interface technology to which an account holder presents biometrics, typically in conjunction with a payment card, for purposes of carrying out a financial transaction, or for enrolling their credential for future use in such transaction.

3.37
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, etc.

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]

3.38
presentation attack detection
PAD
automated determination of a presentation attack

Note 1 to entry: PAD cannot infer the subject's intent. In fact, it may be impossible to derive that difference from the data capture process or acquired sample

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

3.39
re-enrolment
process of establishing a new biometric reference for a biometric data subject already enrolled

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

Note 2 to entry: For example, re-enrolment may be required as a result of performance degradation due to major changes in the system or biometric characteristics.

[SOURCE: ISO/IEC 2382-37:2017, 3.5.13] modified by deleting "in the biometric enrolment database"

Note 3 to entry: See also *biometric enrolment* (3.5) and *initial enrolment* (3.31).