INTERNATIONAL STANDARD

ISO 19092

Second edition
2023-03

Financial services — Biometrics — Security framework

Services financiers — Biométrie — Cadre de sécurité

STANDARDSISO.COM : Click to view the full PDF of ISO 19092:2023

Reference number
ISO 19092:2023(E)

© ISO 2023

STANDARDSISO.COM : Click to view the full PDF of ISO 19092:2023

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
Website: www.iso.org

Published in Switzerland

© ISO 2023 – All rights reserved

Contents

Page

STANDARDSISO.COM : Click to view the full PDF of ISO 19092:2023

© ISO 2023 – All rights reserved

STANDARDSISO.COM : Click to view the full PDF of ISO 19092:2023

© ISO 2023 – All rights reserved

STANDARDSISO.COM : Click to view the full PDF of ISO 19092:2023

© ISO 2023 – All rights reserved

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.

STANDARDSISO.COM : Click to view the full PDF of ISO 19092:2023

© ISO 2023 – All rights reserved

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.

STANDARDSISO.COM : Click to view the full PDF of ISO 19092:2023

© ISO 2023 – All rights reserved

STANDARDSISO.COM : Click to view the full PDF of ISO 19092:2023

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.

STANDARDSISO.COM : Click to view the full PDF of ISO 19092:2023

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 2023 – All rights reserved

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.]

STANDARDSISO.COM : Click to view the full PDF of ISO 19092:2023

© ISO 2023 – All rights reserved

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.]

STANDARDSISO.COM : Click to view the full PDF of ISO 19092:2023

© ISO 2023 – All rights reserved

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.]

STANDARDSISO.COM : Click to view the full PDF of ISO 19092:2023

© ISO 2023 – All rights reserved

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]

STANDARDSISO.COM : Click to view the full PDF of ISO 19092:2023

© ISO 2023 – All rights reserved

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

STANDARDSISO.COM : Click to view the full PDF of ISO 19092:2023

© ISO 2023 – All rights reserved

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

STANDARDSISO.COM : Click to view the full PDF of ISO 19092:2023

© ISO 2023 – All rights reserved

3.43
threshold
numerical value (or set of values) at which a decision boundary exists

[SOURCE: ISO/IEC 2382-37:2022, 37.03.36]

3.44
token service provider
TSP
entity which translates primary account numbers into payment tokens and vice versa

3.45
trusted domain
TD
secure physical or logical area within a given technology providing confidentiality, integrity or authentication services to an application

4 Abbreviated terms

API	application programming interface
ATM	automated teller machine
DSV	dynamic signature verification
HSM	hardware security module
MAC	message authentication code
MPBP	mobile device point of biometric presentation
PAN	primary account number
POI	point of interaction
SCR	secure card reader

5 Biometrics in financial service context

5.1 General

To understand the security perspective of this document, it is useful to compare the use of biometrics in financial transactions with use of a PIN.

Some similarities are as follows:

a) The reference against which the biometric sample is compared is required to be enrolled in advance for the identity of the associated individual, in an analogous manner to a PIN.

b) Currently, biometrics for authentication is mostly used in verification mode, similar to PINs, and not in identification mode. That is, the customer presents their biometric characteristic(s), together with their identity, which is compared 1:1 against an enrolled reference that is looked up based on the claimed identity. Emerging though, are identification-based solutions where the biometric characteristic(s) alone is presented to identify the customer (and their payment credentials) from a "gallery" of customers. Obviously, biometrics is very convenient compared to the potential difficulty or inconvenience of remembering or entering a PIN.

c) For an enrolled customer, presentation of a biometric characteristic(s) can suffice for the transaction to be authorized in an analogous manner to a PIN.

STANDARDSISO.COM : Click to view the full PDF of ISO 19092:2023

© ISO 2023 – All rights reserved

d) Rules for accepting or declining a transaction beyond the decision rules on the result of biometric comparison may be similar or identical to those for PIN.

e) Much of the system infrastructure, except for very specific aspects on biometric processing, is almost identical.

Some notable differences are as follows:

— Unlike PINs, biometric characteristics such as facial images, voice or fingerprints are not secrets. Rather, they are public characteristics of the individual which, with adequate safeguards such as presentation attack detection, are considered sufficiently unique and secure for use in financial transaction authentication, potentially in place of a PIN.

— PIN security relies on, among other things, the use of secure keypad-based PIN-entry technologies and methodologies, and on cryptographic protection of PIN values as they traverse financial authentication systems. Biometric security relies on, among other things, the use of presentation-attack-resistant technologies, potentially augmented by secure biometric capture technologies, and on cryptographic protection of biometric data as it traverses financial authentication systems.

— From a convenience perspective, PIN authentication relies on user memory. Biometric authentication does not.

— Compromised PINs can be replaced in order to reinstate trusted transaction usage; biometric characteristics cannot be changed upon compromise; biometric solutions rely on reliable presentation attack detection.

— While both PIN and biometric authentication processes have non-zero error rates, the added complexity and variability in biometric capture, processing and comparison means biometric solutions are potentially more vulnerable to accuracy and reliability dependencies.

— There are users for whom a particular biometric will not work or is not feasible. Examples include manual labourers with worn fingerprints or people wearing face masks.

— The capture of biometric characteristics may be more susceptible to environmental conditions (e.g. lighting, noise) than the capture of PINs

— Biometric capture under optimum conditions potentially offers usability dividends that PIN cannot, for example contactless authentication via facial recognition.

— Users may have privacy concerns in addition to security concerns about their biometric data.

Arising from these observations, the risk mitigations for biometric authentication set out in this document are focused on:

— identifying biometric-specific security vulnerabilities and addressing each with suitable controls;

— achieving the adequate biometric presentation attack detection while recognizing the challenges this presents;

— securing point of biometric presentations (PBPs) to at least the level for PIN entry;

— ensuring biometric authentication processes mitigate risks to at least the level of PIN-based authentication processes;

— ensuring biometric data handling and transmission is secured to at least the same level as for PIN-based authentication systems;

— ensuring that all other aspects of a biometric authentication achieve a comparable level of security to PIN-based authentication.

STANDARDSISO.COM : Click to view the full PDF of ISO 19092:2023

© ISO 2023 – All rights reserved

5.2 Generic security considerations

Given the very large number of implementation and new-technology possibilities available to financial biometric authentication adopters, the perspective of this document is:

a) to identify business and technical building blocks likely to be common to all such deployments;

b) to identify the communications paths between those building blocks;

c) to assess the vulnerabilities of those domains and communications paths to security threats;

d) to recommend controls to address risks arising from such vulnerabilities and threats.

It is necessarily the case that some security requirements listed in this document will be relatively general in nature. This consideration is especially pertinent due to the proliferating use of personal mobile devices as virtual payment instruments, and in some cases as merchant terminals.

Virtual card implementations mimic the behaviour of contactless smart cards. Available biometric extensions to these implementations are biometric authentication prior to virtual card use or transaction authorization.

Virtual payment terminal implementations mimic the behaviour of traditional secure merchant payment devices. Available biometric extensions for these implementations are:

— user log-on authentication prior to virtual card use;

— biometric transaction authentication using secure biometric reader (SBR) attachment.

Card acceptance during biometric authentication on such personal merchant devices presents additional security challenges, but that topic is not directly addressed by this document.

5.3 Personal device vulnerabilities and controls strategy

As indicated in 5.2, this document provides security guidelines aimed at addressing the security vulnerabilities of personal devices used as PBPs for biometric authentication. Such devices almost universally do not achieve high levels of protection of the biometric data, in part because of their general-purpose computing nature, particularly exposed to fast attack propagation via the internet.

A successful attack against an individual SCD is, by definition, time-consuming and typically has no or very limited prospect of immediate propagation to the population of similar SCDs.

A successful internet-leveraged attack against an individual personal device, while possibly time-consuming to construct in the first instance, may have the potential for simultaneous propagation to a large number of devices. The controls strategy for such devices is required to, among other factors, aim to mitigate this attack propagation risk.

Usage context for personal devices is also important for security. The opportunity for unobserved tampering attacks is higher than traditional payment contexts.

5.4 Biometric verification versus biometric identification

This document distinguishes between biometric verification and biometric identification.

Biometric verification compares an individual's biometric sample with stored biometric reference on a 1:1 basis, closely analogous to a PIN-based system and indexed by a simultaneously presented credential such as a payment card.

Biometric identification matches an individual's biometric with stored biometric references without reliance on accompanying identity information. An example is an account holder paying on the basis of facial recognition in a mass transit system.

STANDARDSISO.COM : Click to view the full PDF of ISO 19092:2023

© ISO 2023 – All rights reserved

6 Biometric modalities and core systems

6.1 General

Biometric recognition leverages the fact that certain physiological or behavioural characteristics can distinguish one person from another.

Such characteristics, also known as biometric modalities, include fingerprints, voiceprints, iris patterns, facial image, vein patterns, signatures and keystroke dynamics. A brief description of these techniques is given in 6.2, noting that other viable modalities may exist.

Biometric technology includes the capture and the comparison of these biometric characteristics. The digital representations of these characteristics are used to confirm the identity of an individual. A typical biometric authentication process consists of the following basic steps:

a) capturing the biometric data;

b) evaluating the quality of the captured biometric data and recapturing it if necessary;

c) processing the captured biometric data;

d) comparing the processed biometric data with one or more previously enrolled biometric references to determine if a match exists; this comparison can be done for biometric verification or biometric identification.

The biometric data life cycle consists of the following:

— Enrolment: confirming the identity of the participant and enrolling them in the system.

— Establishment of biometric reference: the capture and storage of one or more biometric samples that will be used in the biometric comparison process.

— Use of biometric references in the biometric comparison process while verifying or identifying a participant.

— Updating a biometric reference through re-enrolment or updating of the biometric data.

— Termination: removal or deactivation of biometric reference from any operational system.

— Archiving: the process of securely storing biometric data for non-operational purposes.

6.2 Modalities of biometrics

6.2.1 General

The following subclauses (6.2.2 to 6.2.9) discuss a selection of biometric modalities and conditions that can impact the suitability for their use for a given purpose.

6.2.2 Fingerprint

Friction ridges and valleys on an individual's fingertips are considered unique to that individual. For over one hundred years, law-enforcement agencies have been classifying fingerprint images into one of several main types and sub-types (i.e. fingerprint patterns such as loops, whorls and arches) as well as determining identity by comparing key points of ridge endings and bifurcations. Fingerprints appear unique for each finger on the same hand, as well as between identical twins.

Most modern fingerprint-matching technology focuses on the unique points within the finger image, the minutiae. These minutiae are the points where individual friction ridges branch apart (bifurcate) or end. Imaging algorithms extract the minutiae and create a proprietary template that codes these minutiae. Pattern-matching systems are based on overall ridge flow as opposed to minutiae. Systems can also analyse the finger's tiny sweat pores or the number of ridges between two singular points (such

STANDARDSISO.COM : Click to view the full PDF of ISO 19092:2023

© ISO 2023 – All rights reserved

as the cores and the delta). Fingerprint biometrics is capable of both verification and identification. Recently, deep learning technology has been widely used for increasing biometric recognition, including low-quality fingerprint classification and liveness detection.

Conditions that may affect the prints of different individuals and reduce the quality of image capture include dirty, dry or cracked prints. Age, gender and body size are also found to have an impact on the quality of finger images, as well as the placement (rotation, shift and pressure) of the finger on the scanner (see the ISO/IEC 19795 series and ISO/IEC TR 24714-1). The public may see the historical use of fingerprinting by government law-enforcement organizations as a negative, although the capture of the fingerprint is generally regarded as non-invasive and widely performed through personal devices such as mobile phones. Contactless fingerprint capture as a technology that alleviates some of the issues with respect to placement of the finger and also acquisition of three-dimensional fingerprints can be regarded as recent technologies.

6.2.3 Voice biometrics

Voice biometrics (also called "speaker recognition") models the acoustic features of speech that have been found to differ between individuals yet remain stable over time for a single individual. These acoustic patterns reflect both anatomy (e.g. size and shape of the throat and mouth) and learned behavioural patterns (e.g. voice pitch, speaking style).

Speaker recognition systems can employ either of two styles of spoken input: text-dependent and text-independent speech. Text-dependent systems ask users to repeat specific words, phrases or numbers where text-prompted input can be used to protect from replay attacks using recording voices. Text-independent systems input is free-flowing speech.

Applications of speaker identification by law-enforcement agencies typically use text-independent input because it does not require enrolment or input of specific words. Input speech is "digitized" to create a series of numbers. From these numbers, a reduced set of "features" is extracted mathematically. Voice biometrics is commonly used for verification, but rarely for identification. Recently, deep learning technology has been widely used for automatic feature extraction and recognition.

Ambient noise levels can be an impediment to the collection of voice samples. Voice changes due to ageing also need to be addressed by voice biometrics systems; biometric reference adaptation can be employed to evolve the voice template along with changes in the verified speaker's voice.

6.2.4 Iris biometrics

The iris is the round-coloured portion of the eye behind the cornea and surrounds the pupil. A person's iris pattern is unique and remains unchanged throughout adulthood. Iris recognition has been successfully used in access control applications without the need for any form of identification or claim of identity by the data subject. In most implementations, a grayscale image of the iris is acquired in the near-infrared spectrum to maximize detail in eyes of all colours.

The computer algorithms unwrap these images to form a rectangular matrix of pixels over which a smaller filter is placed in multiple locations. The filter represents a smooth wave with a frequency and direction (see ISO/IEC 19790). This is usually done by Daugman's representation. Recently, deep learning technology has been widely used for automatic feature extraction and recognition.

To ensure pupil constriction to maximize the area of the iris, acquisition should be done in a well-lit environment. That is, sensors often have a light source that lights up the eye before capture to improve iris capture area. Non-patterned contact lenses and glasses do not interfere significantly with image capture. Sunglasses, however, should not be worn, as they can affect the capture process.

6.2.5 Face biometrics

The human face plays an important role in conveying the identity of an individual. Some face biometrics solutions utilize images captured in the visible spectrum using standard camera technology. Near-infrared camera is also adopted to minimize the visible spectrum and lightening interference. An

STANDARDSISO.COM : Click to view the full PDF of ISO 19092:2023

© ISO 2023 – All rights reserved

alternative approach, known as facial thermography, uses an infrared camera to capture the unique heat emission patterns made by people's faces. The multispectral visible and infrared systems extract facial features from captured facial images.

Feature extraction of facial images in the visible spectrum includes machine learning, such as principal component analysis and local feature analysis. Principal component analysis, or the "eigenface" technique, models a particular face as a weighted combination of other "basis" faces. The set of basis faces is constructed by collecting many face images, then mathematically determining the set that optimally models them all. Deep learning-based systems are being used where a feature vector is extracted and then compared using a specific distance metric such as Euclidean distance or cosine similarity.

Three-dimensional maps of the face can be created through either projecting a pre-calibrated grid of pattern or using a stereo camera system. The created three-dimensional maps of the face can be used for pose-invariant face recognition. Face biometrics is capable of both verification and identification.

Challenges for facial identification include reducing the impact of changes in pose, expression, hairstyle, facial hair, makeup, different cameras and lighting. Age, gender and ethnicity are also found to have an influence on the quality of face recognition by the scanner. Some facial biometrics systems may require a stationary or posed user in order to capture the image, though some systems use motion imagery. All systems process the images to detect a person's head and locate the face automatically. Major advantages of facial identification are that it is non-intrusive, hands-free, continuous authentication and accepted by most users. The intrinsic difficulty to distinguish between identical twins in the visual spectrum can be overcome by adopting multi-modal biometrics, such as the vein pattern found in the infrared spectrum on the forehead or iris.

6.2.6 Signature biometrics

Hand-written signatures can be identified from the way the signature looks and the way the hand of the signer moves during the signing. Signature recognition based upon the biometric characteristics related to movement of the hand is referred to as DSV. A number of characteristics can be extracted and measured by DSV. For example, the time taken to sign, the velocity and acceleration of the signature, the pressure exerted when holding the pen and the number of times the pen is lifted from the paper can all be extracted as distinctive characteristics. DSV is not based solely on the static image, so even if a signature is traced, a forger would need to know the dynamics of that signature. Electronic pens, tablets or both can be used to capture the signature biometrics. Digitized signatures are generally used in verification as opposed to identification mode. Since the execution of a signature is strongly influenced by behavioural and social conditions, two repetitions of a signature from the same person never have an identical dynamic. So, to permit the effect of intrapersonal variability without deteriorating the performance of distinguishing other persons is crucial.

6.2.7 Vein biometrics

Vein authentication uses the pattern of blood vessels in the subcutaneous tissue of the human body to discriminate between individuals. A vein pattern is read using near-infrared light. The blood vessels absorb infrared light more than the surrounding tissue and appear darker in the acquired image. The shaded part is extracted from the captured image as the blood vessel pattern of the vein using image processing technology. The resulting blood vessel pattern is compared using vessel structure features such as directions and bifurcations or using the pattern itself.

A blood vessel pattern of a hand, such as that of a palm, the back of a hand or a finger, are used for authentication because such parts of the hand are easy to present to a sensor, and various products have been developed for such hand parts. Because the products have many functions to support and guide users in proper usage, such as detection of hand position based on image-processing technology, high usability is achieved and the accuracy of authentication is very stable. Since the blood vessel pattern used by vein authentication is information that is hidden in a body, it is generally not known by others in typical usage environments, and therefore forgery is difficult. Vein biometrics can be used in conjunction with hand geometry.

STANDARDSISO.COM : Click to view the full PDF of ISO 19092:2023

© ISO 2023 – All rights reserved

In actual products employed by ATMs, the parts of the body chosen (e.g. palm, fingers, wrist and the back of the hands) are the parts where a user can easily present the blood vessel pattern to the sensor. Cold temperatures cause vein constriction, therefore outdoor use can be problematic.

6.2.8 Palm print biometrics

Palm prints show a complex set of skin lines and creases that is unique to identify an individual. Palm print authentication uses the friction ridges containing minutiae points found on the palm. These can be captured using optical techniques. Other palm print biometrics based on the hand geometry and palm print crease have been developed. This can support a kind of multi-modal authentication using the palm print lines and hand geometry. Considerations for use of minutiae are similar to those of fingerprints. Recently, contactless palm-print recognition based on the deep learning for high performance has been used in various circumstances.

6.2.9 Keystroke biometrics

Keystroke dynamics analyse typing rhythm. This applies to entering the method of character entries such as smartphones or keyboards. It measures the times between keystrokes and the hold time of keys.

An individual's keystroke dynamics evolve over time as they learn to type and develop their own distinctive typing habits. The algorithms may need to cope with subjects becoming distracted or tired during the course of the keying works. So, this is often used in conjunction with primary biometric traits to further improve performance. This can support a kind of continuous authentication when the individual is connected.

6.3 Biometric system and its supporting systems

6.3.1 Overview

The following subclauses provide conceptual illustrations of the core technical building blocks of a biometric authentication system, set against the following four main usage scenarios:

a) registration;

b) enrolment;

c) transaction usage with accompanying credentials;

d) transaction usage without accompanying credentials.

Attendant processes may include biometric reenrolment, reference refinement and termination.

The core systems underlying these usage scenarios are typically as follows:

— identity management system;

— account management system;

— biometric system

  — capture subsystem;

  — feature extraction subsystem;

  — storage subsystem;

  — comparison subsystem;

STANDARDSISO.COM : Click to view the full PDF of ISO 19092:2023

© ISO 2023 – All rights reserved

- decision subsystem;
- transaction authorization system;
- credential management system.

Note that the building block descriptions given in this clause are largely independent of implementation specifics: multiple individual functions can be grouped together on one platform or can be distributed across multiple platforms or multiple locations as determined by the biometric authentication system operator.

6.3.2 Core systems

6.3.2.1 Identity management system

The identity management system is the first PBP of a prospective account holder when establishing an account which may be used with biometric authentication. Such a system could be biometric-agnostic.

The identity management system embodies the procedures and interfaces by which an account holder is registered with a financial biometric authentication system operator – typically an issuer – prior to biometric enrolment, and for the purpose of account management. The degree to which the identity management system is directly cognizant of biometric usage depends on the implementation, noting only that enrolled biometric references for financial authentication are always coupled with an underlying registered account.

6.3.2.2 Account management system

An account management system exists for all financial biometric authentication scenarios. It is normally located in the issuer domain and represents the processes and data sets involved in managing the financial accounts of authentication system customers, closely coupled to or embodying identity management functions.

6.3.2.3 Biometric system

6.3.2.3.1 Capture subsystem

A biometric capture subsystem exists at all PBPs except identity management where, nonetheless, it might be co-located for enrolment. It comprises sensors to capture the biometrics along with initial sample conditioning logic such as might suppress ambient noise or otherwise adapt the sensor to ambient conditions.

6.3.2.3.2 Feature extraction subsystem

A biometric feature extraction subsystem takes the output of the preceding capture stage and extracts relevant biometric features, known as a biometric reference, ready for storage in the enrolment phase, or for comparison in the transaction usage case.

This subsystem might be co-located in the capture PBP technology, or at some separate node linked via a communications path with the capture PBP.

6.3.2.3.3 Storage subsystem

A biometric storage subsystem is a subsystem responsible for the storage and retrieval of biometric references. It might be a central database containing the reference of many account holders, or the set of biometric references applying to a single account holder stored on a smart card.

STANDARDSISO.COM : Click to view the full PDF of ISO 19092:2023

© ISO 2023 – All rights reserved

6.3.2.3.4 Comparison subsystem

A biometric comparison subsystem takes the output of the preceding processing stage, along with accompanying account identifier in the case of verification, and carries out a comparison with the associated biometric reference, generating either a match/non-match result or a score that indicates the degree to which the references match with the result submitted to the biometric decision subsystem. For verification, the reference will be found by lookup, keyed by the accompanying credential such as PAN. For identification, the candidates are obtained by scanning the entire available set of references.

This subsystem might be co-located with preceding subsystems or at some separate system node.

6.3.2.3.5 Decision subsystem

A biometric decision subsystem takes the output of the preceding comparison stage, along with any accompanying account identifiers and any other decision-conditioning rules, and outputs a pass or fail result for consumption by the following transaction authorization subsystem.

This subsystem might be co-located with preceding subsystems or at some separate system node.

6.3.2.4 Transaction authorization system

The transaction authorization system, typically located in the issuer environment, takes the output of the preceding biometric decision subsystem during a financial transaction and makes the decision as to whether the transaction proceeds, communicating that back to the PBP.

This system is highly interdependent with the account management system. As an example, for a payment authorization request, the transaction authorization system would interrogate the account management system to establish funds sufficiency and might post the transaction amount to the account ledger upon completion of a successful authorization.

6.3.2.5 Credential management system

The credential management system is located in the issuer environment and issues and handles authentication credentials. Among the registration steps, the credential management system issues authentication credentials for account holders. The authentication credential might take the form of a physical smart card, with or without inherent biometric capability, an account number, a biometric card enrolment passcode or a PIN to be used in addition to a biometric or as a fallback authentication method.

6.3.3 Core biometric authentication usage scenarios

6.3.3.1 General

The following subclauses illustrate the core generic usage scenarios involving the previously described biometric systems. These illustrations assume a pre-existing payment systems environment comprising back-end acquiring, issuing, identity management and account management systems. Specific technology choices and considerations are furnished in Clause 10.

Figure 1 defines the symbols used to identify different generic PBP types in the forthcoming diagrams:

a) Public device PBPs, where the biometrics of multiple financial account holders will be presented to a common public interface.

b) Personal card PBPs, where biometric capture and further biometric processing occur on a smart card payment instrument belonging to an account holder.

c) Personal device payment instrument PBPs, where a personal (typically mobile) device is used for biometric capture, and potentially further biometric processing.

STANDARDSISO.COM : Click to view the full PDF of ISO 19092:2023

© ISO 2023 – All rights reserved

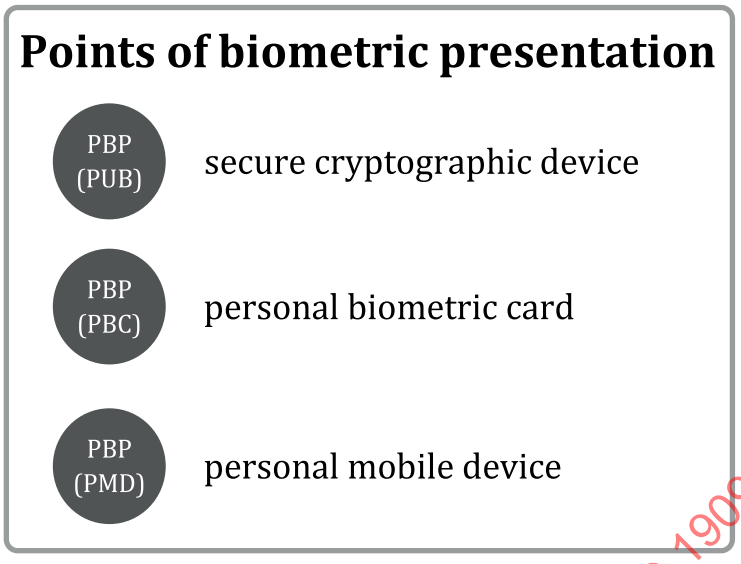


Figure 1 — Points of biometric presentation – legend

STANDARDSISO.COM : Click to view the full PDF of ISO 19092:2023

6.3.3.2 Registration scenario

Registration (see Figure 2) is the process by which a prospective user of biometric authentication – hereafter referred to as the account holder – identifies themselves to a financial institution and establishes an account (if not already having such an account) prior to enrolling their biometrics. Indicative registration steps are as follows:

a) The user presents evidence of identity and establishes an account with a payment instrument issuer.

b) The issuer confirms the identity of the applicant, establishes an account and issues authentication credentials. Such credentials can include:

- a physical smart card, with or without inherent biometric capability;
- an account number;
- a biometric card enrolment passcode;
- a PIN where that is to be used in addition to a biometric or as a fallback authentication method.

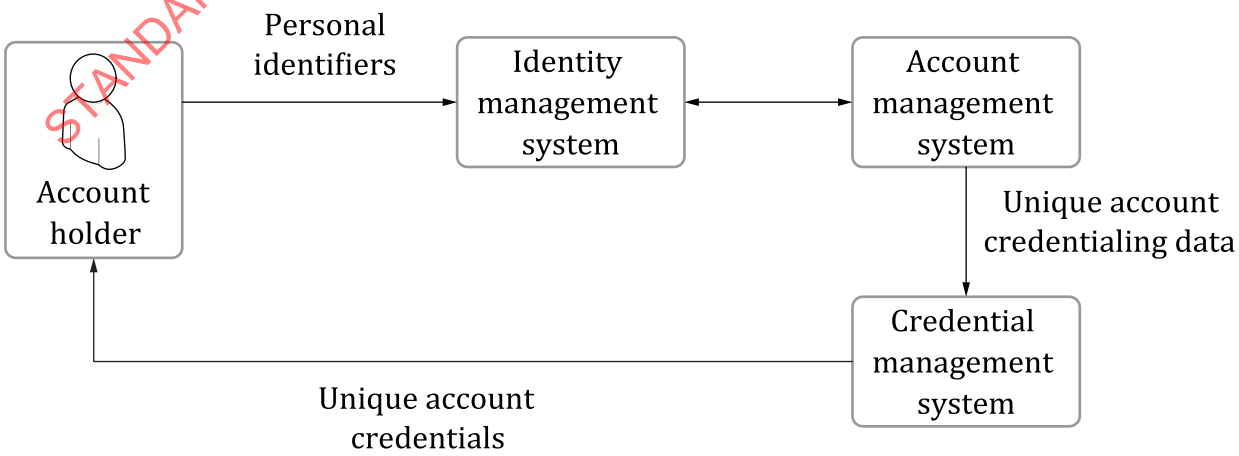


Figure 2 — Core systems – registration

© ISO 2023 – All rights reserved

6.3.3.3 Enrolment scenario

Enrolment is the process of recording a biometric reference to be used in the biometric comparison process carried out during transaction usage, see Figure 3. An identity management system linking the account holder with the biometric system may or may not exist depending on the financial service system. The location and nature of the PBP technology and sample processing technology is implementation-dependent, as is the final storage location of the biometric reference, which can be within or out of the biometric system depending on the implementation, see later use case architectures.

Note that the enrolment process may entail a biometric identification search stage to establish whether a given identity is already enrolled.

Note also that there is a closely related re-enrolment (reference refresh) scenario described 10.8 which employs the same subsystems.

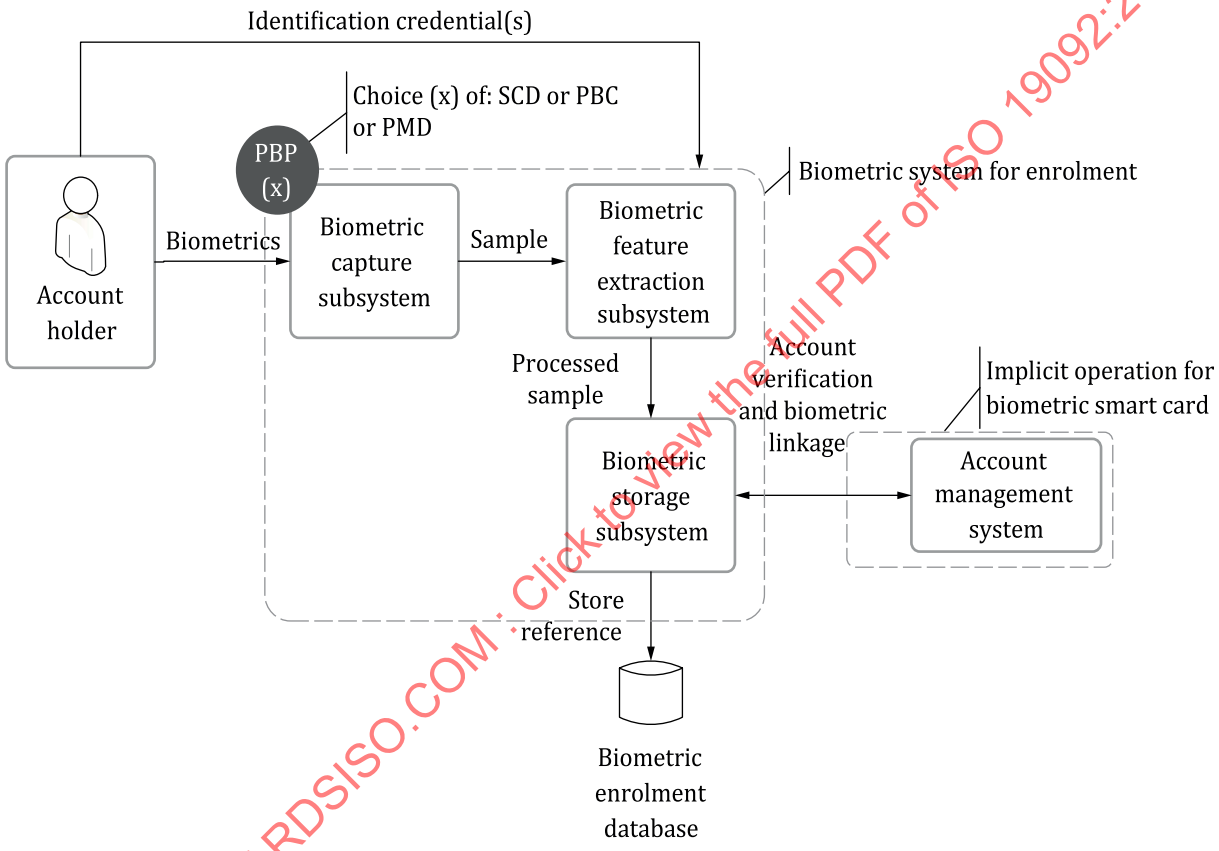


Figure 3 — Core systems – enrolment

STANDARDSISO.COM : Click to view the full PDF of ISO 19092:2023

6.3.3.4 Transaction usage scenarios

6.3.3.4.1 Overview

The key differences between biometric verification and biometric identification are described in 5.4. Characteristic implementations addressing those differences are illustrated in the following examples.

6.3.3.4.2 Authentication using biometric verification

Biometric financial transaction authentication most commonly relies on biometric verification.

In the example in Figure 4, a credential identifying the account holder and one or more associated biometric characteristics are presented to a PBP to initiate the authentication process.

© ISO 2023 – All rights reserved

Biometric features are captured, extracted and passed as a biometric sample to the biometric comparison subsystem, the latter also being supplied with the biometric reference associated with the identification credential. Sample and reference are compared, with the outcome forwarded to the biometric decision-making subsystem. The decision result, claimed identity and other information, such as transaction amount requested for authorization, are forwarded to the account management for further processing.

Note that, contingent on biometric decision criteria being met, offline transaction authorization is feasible for biometrically capable cards or mobile devices where security policy permits.

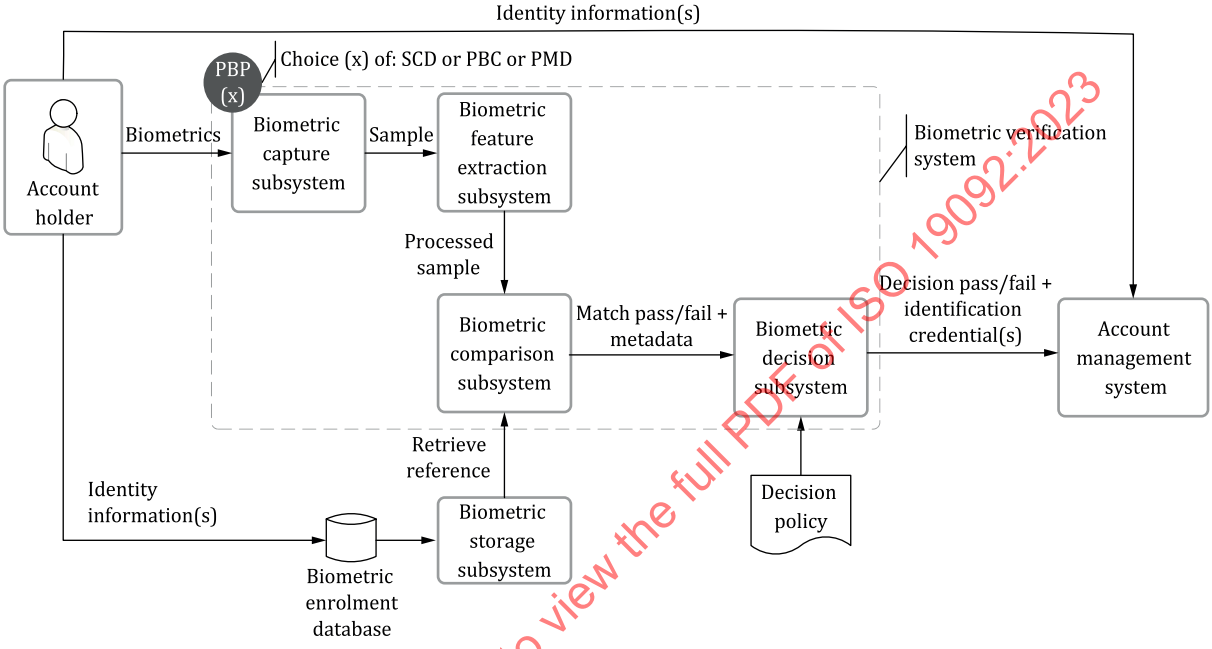


Figure 4 — Core systems – verification

6.3.3.4.3 Authentication using biometric identification

Transaction authentication using biometric identification provides a potential alternative to transaction authentication using biometric verification.

In this scenario (see Figure 5) no separate identity credential is employed. On presentation of a biometric sample, the comparison subsystem attempts to establish the identity of the account holder by searching a database of stored references, looking for a closest reference. Where a match is found, the result is forwarded to the decision subsystem, along with the inferred identity of the account holder, with the outcome of the decision process and associated identity forwarded to the account management system for further processing. Offline transaction authentication is infeasible in practical deployments of authentication using biometric identification.

STANDARDSISO.COM : Click to view the full PDF of ISO 19092:2023

© ISO 2023 – All rights reserved

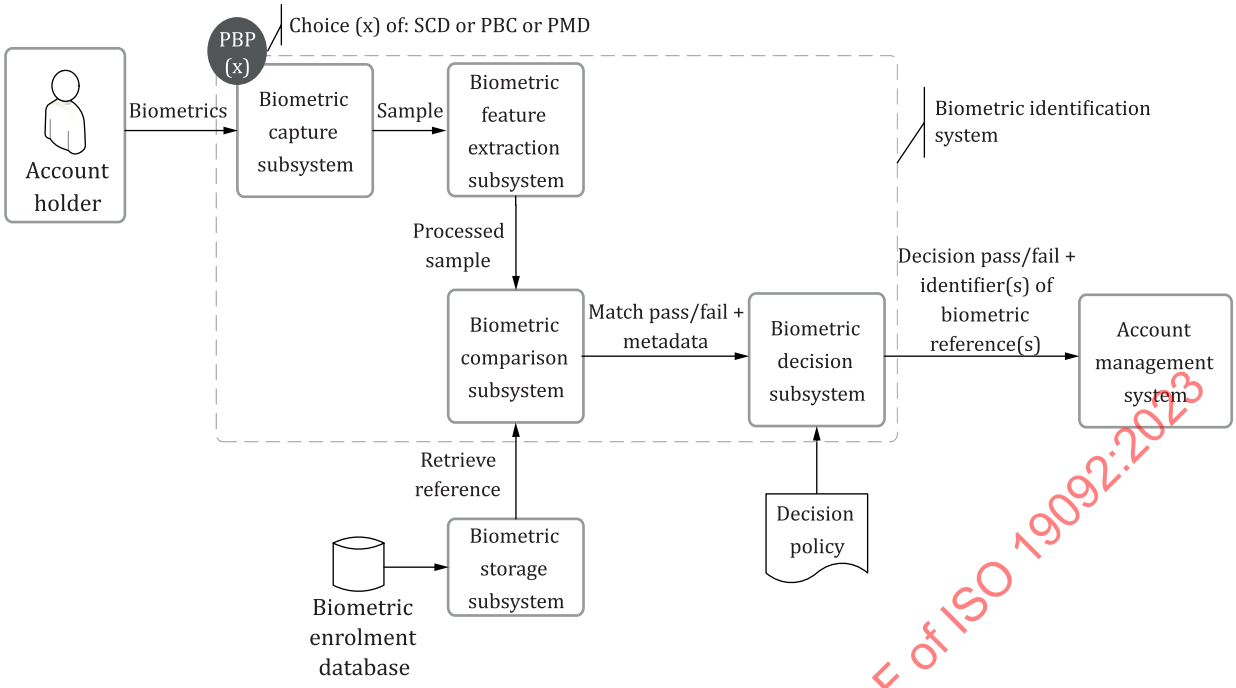


Figure 5 — Core systems – Identification

STANDARDSISO.COM : Click to view the full PDF of ISO 19092:2023

7 Financial biometric authentication systems — usability considerations

7.1 General

The following are core considerations in designing and operating a biometric system:

— Properties of biometric modalities.

— Recognition performance: the ability of the system to reliably authenticate or identify users. FMR and FNMR – the rates at which incorrect decisions are made – are crucial factors.

— Recognition performance evaluation: measurement of the ability of a system to provide accurate results within an acceptable time limit.

— Presentation attack resistance.

— Interoperability: the degree to which one biometric authentication deployment may interoperate with another such deployment.

7.2 Properties of biometric modalities

The viability of biometric authentication for financial transactions relies on account holder identity being associated with one or more distinguishing, repeatable biometric features to a high degree of certainty. In designing and operating such a system, the following properties of biometric modalities should be considered:

— universality: the applicability of the modality to all members of the target population;

— distinctiveness: the ability of the modality to differentiate each member of the target population;

— acceptability: the willingness of members of the target population to use the specified biometric characteristic for a given application;

— stability: the resistance of a biometric characteristic to change over time;

© ISO 2023 – All rights reserved

— insensitivity: the consistency of a biometric characteristic across varying capture environments;

— accessibility: the ease with which a biometric characteristic can be captured by a sensor;

— vulnerability: the level of immunity of a biometric characteristic to presentation attacks.

NOTE 1 The resistance to fraud relating to the use of a biometric characteristic depends on presentation attack detection and affects the security of the biometric system.

NOTE 2 The distinctiveness of each modality is different. For example, iris biometrics can cover a larger target population than vein biometrics.

7.3 Properties and evaluation of biometric system

7.3.1 Recognition performance

Biometric techniques are subject to statistical errors such that impostors may be authenticated and legitimate users rejected. Recognition performance measures the accuracy of biometric verification and identification expressed in terms of error rates such as false match rate (FMR), false non-match rate (FNMR), false-positive identification rate (FPIR) and false-negative identification rate (FNIR).

The probability that a biometric system fails to reject an impostor in a 1:1 verification attempt, or incorrectly identifies an individual in a 1:*N* identification attempt, is reflected in the system's FMR and FPIR, respectively.

The probability that a biometric system fails to verify an enrolled individual in a legitimate 1:1 verification attempt, or fails to identify an enrolled individual in a 1:*N* identification attempt, is reflected in the system's FNMR and FNIR, respectively.

The biometric modalities identified in this document are all prone to some level of FMR and FNMR.

A system's FMR and FNMR are inversely related, such that reducing the FMR by adjusting biometric system security settings can result in an increased FNMR, and vice versa. A match or a non-match is typically determined using matching parameters and threshold, which are decided by the biometric policy. A system's FMR and FNMR cannot be independently adjusted. Instead, a threshold is normally selected above which a match is declared and below which a non-match is declared.

Once a match is decided by the comparison subsystem, a decision subsystem typically is used to determine whether the match is accepted based on additional contextual factors, such as:

— prior match history;

— the number of non-matches preceding a match;

— the time taken to achieve a match;

— the security context of the presentation environment.

Most biometric systems allow multiple presentation attempts before rejecting further attempts. For example, an individual may be permitted to present a fingerprint to a scanner up to three times. A common decision policy here is to grant access if any of the three attempts is successful. Under this policy, the system's effective FNMR may be lower than its single-attempt FNMR. That is, the user is more likely to be verified when additional attempts are allowed. Such a decision policy, however, increases a system's effective FMR, giving an impostor multiple chances to try to defeat the system.

Another decision factor can be the number of enrolled biometric references associated with a given user. Many biometric systems acquire two enrolment biometric references from a user, such as from the right and left fingerprints. This mitigates the impact of injuries or other variables that may impair presentation accuracy.

If a system allows a user to verify against more than one biometric reference, the system's effective FNMR may be lower than its single-attempt FNMR. That is, a user is more likely to be verified when

STANDARDSISO.COM : Click to view the full PDF of ISO 19092:2023

© ISO 2023 – All rights reserved

more than one biometric reference exists for that person. Allowing more than one biometric reference, however, increases a biometric system's effective FMR, and provides an impostor with additional matching opportunities.

Other decision policy elements that can impact a system's accuracy include:

— the number of different biometric technologies (e.g. fingerprint, voice) in which the claimant is enrolled;

— the technical sophistication or agility in the comparison process in detecting like or non-like biometric samples, for example in automatically detecting and adapting to different enrolled fingers in successive presentation attempts;

— the use of serial, parallel, weighted or fusion decision logic in biometric systems that cater for more than one biometric reference in the comparison process for a given user.

A biometric system's effective FMR and effective FNMR represent its error rates with all elements of the decision policy taken into consideration. A secure biometric system implementation requires that deployers carefully evaluate the security risks attached to the chosen decision policy for the given technology choices.

7.3.2 Recognition performance evaluation

When evaluating the recognition performance of biometric technology, it is important to understand the different factors that can influence the measured FMR and FNMR. For example, the reported accuracy of different implementations has possibly been measured under different circumstances and thus cannot be directly comparable.

The following factors should be taken into consideration when evaluating recognition performance. (For more detail about biometric performance testing and reporting, see the ISO/IEC 19795 series.)

— Test subject selection: test subjects should be chosen at random from a population that is representative of the people who will use the system in the real application environment, noting that it may not always be feasible for the sample population to fully reflect the target population, including both biographic and demographic factors. For example, if the test group comes from the vendor's employee population, they may differ significantly from the target users in terms of educational level, cultural background and other factors that may influence the performance of the live biometric system.

— Level of training: to avoid introducing bias, test subject training should be as close as possible to that anticipated for users of the real system.

— Threshold setting: match threshold for testing should correspond to those of the production system.

— Verification attempts: the number of verification attempts used in testing should correspond to those of the production system.

NOTE 1 Biometric performance depends upon precise conditions of PBP installation and use and can be subject to considerable variation. A biometric system typically produces statistically different outcomes or decisions for different demographic groups, for example those based on gender, age and race. Refer to ISO/IEC TR 22116 for more detail.

NOTE 2 ISO/IEC 19795-1 provides the principles and framework for evaluating biometric systems in terms of error rates and throughput rates. Metrics for the various error rates in biometric enrolment, verification and identification are specified.

NOTE 3 ISO/IEC 19795-2 provides requirements and recommendations on data collection, analysis and reporting specific to the two primary types of evaluation: technology evaluation and scenario evaluation.

NOTE 4 ISO/IEC TR 19795-3 defines modality-specific testing. It presents methods for determining, given a specific biometric modality, how to develop a technical performance test.

STANDARDSISO.COM : Click to view the full PDF of ISO 19092:2023

© ISO 2023 – All rights reserved

NOTE 5 ISO/IEC 19795-4 prescribes methods for technology and scenario evaluations of multi-supplier biometric systems that use biometric data conforming to biometric data interchange format standards.

7.3.3 Presentation attack detection

A presentation attack entails presentation of a copied, fake or synthesized biometric characteristic to a sensor with the aim of achieving illicit authentication and evading recognition. Examples of such attacks include the use of a gummy finger or glue on finger for fingerprint modalities, facial video, three-dimensional masks or non-permanent make up for face modalities and patterned contact lens for iris modalities.

Presentation attack detection refers to techniques designed to detect and exclude presentation attacks. Like the characteristic they protect, presentation attack detection is subject to errors, both false positive and false negative. False positive indications wrongly categorize bona fide presentations as attacks. False negative indications wrongly categorize presentation attacks as bona fide presentations.

Evaluation of such techniques measures their ability to discriminate fake or artificial presentations from bona fide presentations. The decision to use a specific presentation attack detection implementation depends on the requirements of the given application and almost certainly involves trade-offs between security and efficiency.

Presentation attack detection evaluations focus on the effectiveness of the sensor and associated logic to reject false or doubtful samples. Such tests are frequently based on a collected sample database.

NOTE 1 The ability to carry out effective presentation attack detection can be highly constrained for some implementations such as smart card fingerprint readers.

NOTE 2 ISO/IEC 30107-1 defines terms and establishes a framework for presentation attack detection.

NOTE 3 ISO/IEC 30107-2 defines data formats for use in presentation attack detection.

NOTE 4 ISO/IEC 30107-3 establishes principles and methods for performance assessment of presentation attack detection algorithms and associated mechanisms.

NOTE 5 ISO/IEC 30107-4 establishes a profile that provides requirements for testing biometric presentation attack detection mechanisms on mobile devices with local biometric recognition.

7.3.4 Interoperability

Interoperability of financial biometric authentication systems presents challenges to issuers and acquirers, including the following:

— biometric capture devices – sensor or camera interoperability;

— compatibility of biometric modalities – interoperable issuers must share at least one modality;

— security assurance level compatibility between different biometric modalities and different device vendor implementations for the same modality;

— security assurance level compatibility between different implementation architectures, for example between acquirer- or issuer-managed fully-SCD-based implementations compared to third-party implementations relying on non-SCD mobile devices;

— biometric data format compatibility between entities.

NOTE The ISO/IEC 19794 series and the ISO/IEC 39794 series provide guidance on notionally interoperable data-exchange formats for many common biometric modalities. The ISO/IEC 19795 series provides test guidance applying to those formats.

STANDARDSISO.COM : Click to view the full PDF of ISO 19092:2023

© ISO 2023 – All rights reserved

8 Financial biometric authentication systems – architectures

8.1 Overview

A biometric authentication system consists of a set of hardware and software building blocks and an environment operated or managed by a limited number of payment system participants.

8.2 Conceptual business architecture

Figure 6 provides a conceptual illustration of the most likely entities involved in the deployment and operation of a biometric financial transaction authentication system. These entities are issuers, acquirers, merchants, third parties and account holders. For the purposes of this document, these entities are defined as follows:

a) Issuers: entities holding the accounts of identified individual financial account holders, and responsible for such things as transaction authorization for such user's accounts.

b) Acquirers: entities responsible for acquiring payment transactions from merchant or other terminals and forwarding them for authorization to issuers. This role is increasingly diffuse as new PBP technologies and transaction processing implementations enter the financial technology market.

c) Merchants: individuals or companies requesting payment authorization for goods or services via the biometric authentication system, traditionally via an acquirer.

d) Third parties: entities providing one or more subsystem services in biometric authentication subsystems and payment systems more generally. Potential third parties include:

   — a token service provider (TSP), most frequently in connection with the use of virtualised mobile platform payment instruments;

   — a personal device wallet managing personal device on-platform application provisioning, payment token instantiation, run-time monitoring and mobile transaction functions.

e) Account holders: parties who have a registered account with an issuer and use a biometric to authenticate payment authorization requests towards an issuer.

NOTE This document does not preclude a single entity carrying out more than one of the roles described. For example, a bank can be both issuer and acquirer.

STANDARDSISO.COM : Click to view the full PDF of ISO 19092:2023

© ISO 2023 – All rights reserved

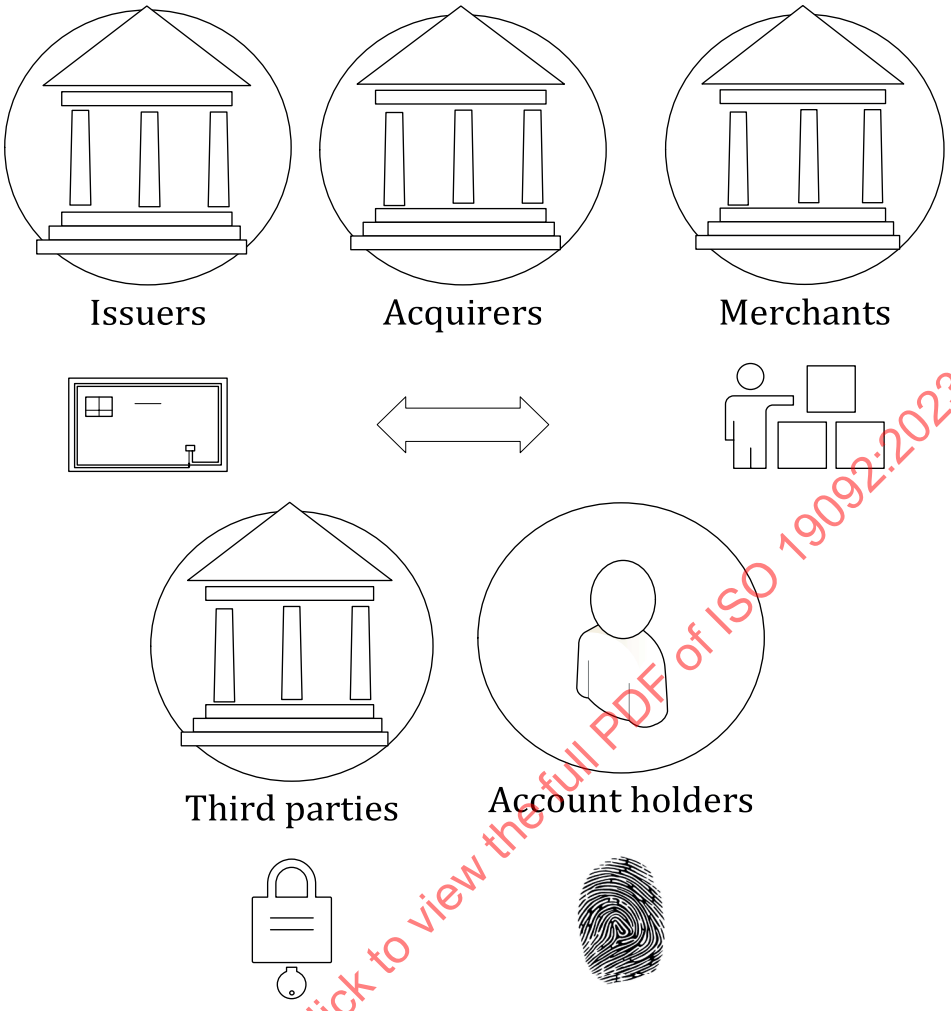


Figure 6 — Biometric system business entities

STANDARDSISO.COM : Click to view the full PDF of ISO 19092:2023

8.3 Technical architecture

This document makes no specific prescriptions for the technical architecture of a biometric authentication system. That is, aside from the axiomatic fact that a biometric must be presented at a PBP and that the system will be built in some fashion from the building blocks described in 6.3, the system's paramount objective is to provide a secure financial transaction authentication process through appropriate technology choices.

8.4 Registration architecture

All biometric enrolment and transaction-time actions presuppose a preceding account holder registration step such as illustrated in Figure 7.

An account holder who intends to use biometric authentication presents personal identifiers to the identity management system. The identity management system verifies the account holder using an existing authentication method. The account management system registers biometric information as one of the unique account credentials. Unique account credentials may include, among other things, such items as PAN, card security codes, address, date of birth and government-issued identity documents.

© ISO 2023 – All rights reserved

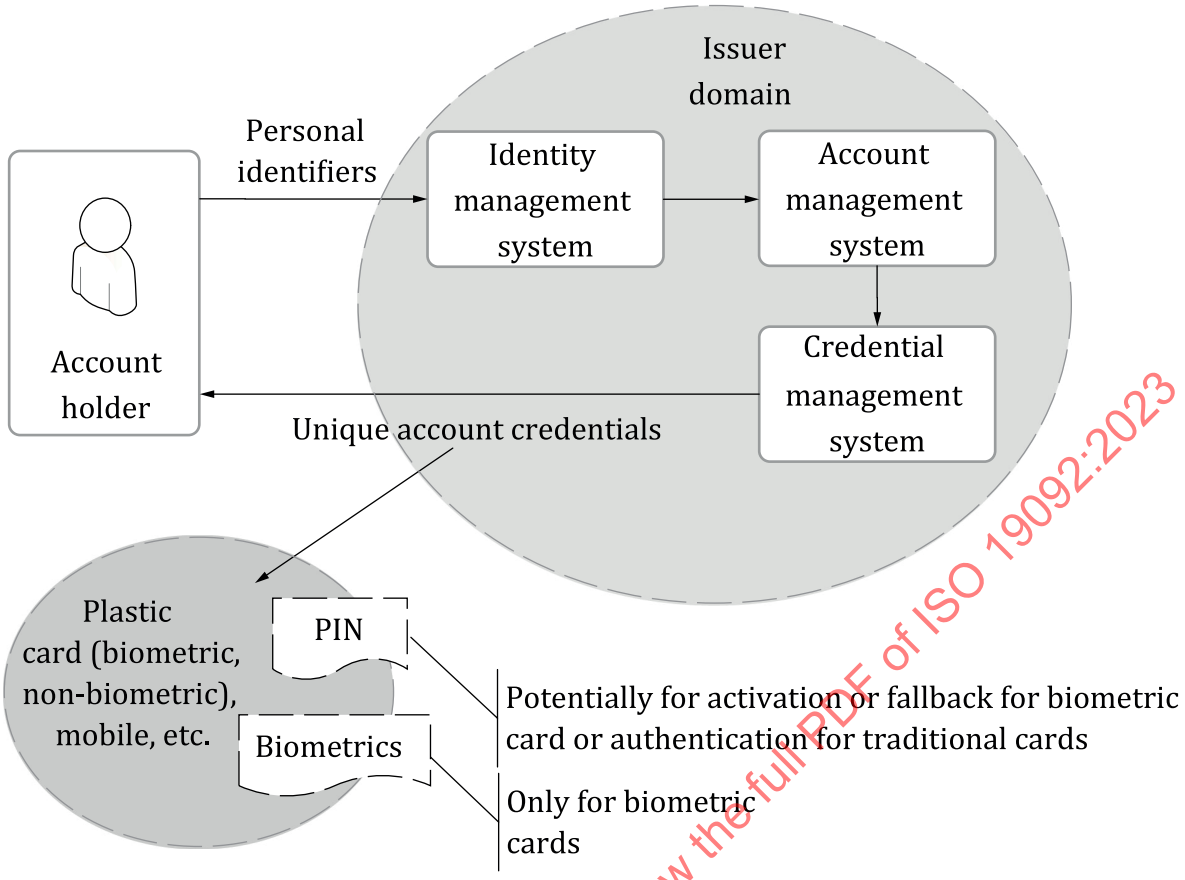


Figure 7 — Conceptual architecture for registration prior to biometric enrolment

8.5 PBP devices and associated biometric authentication architectures

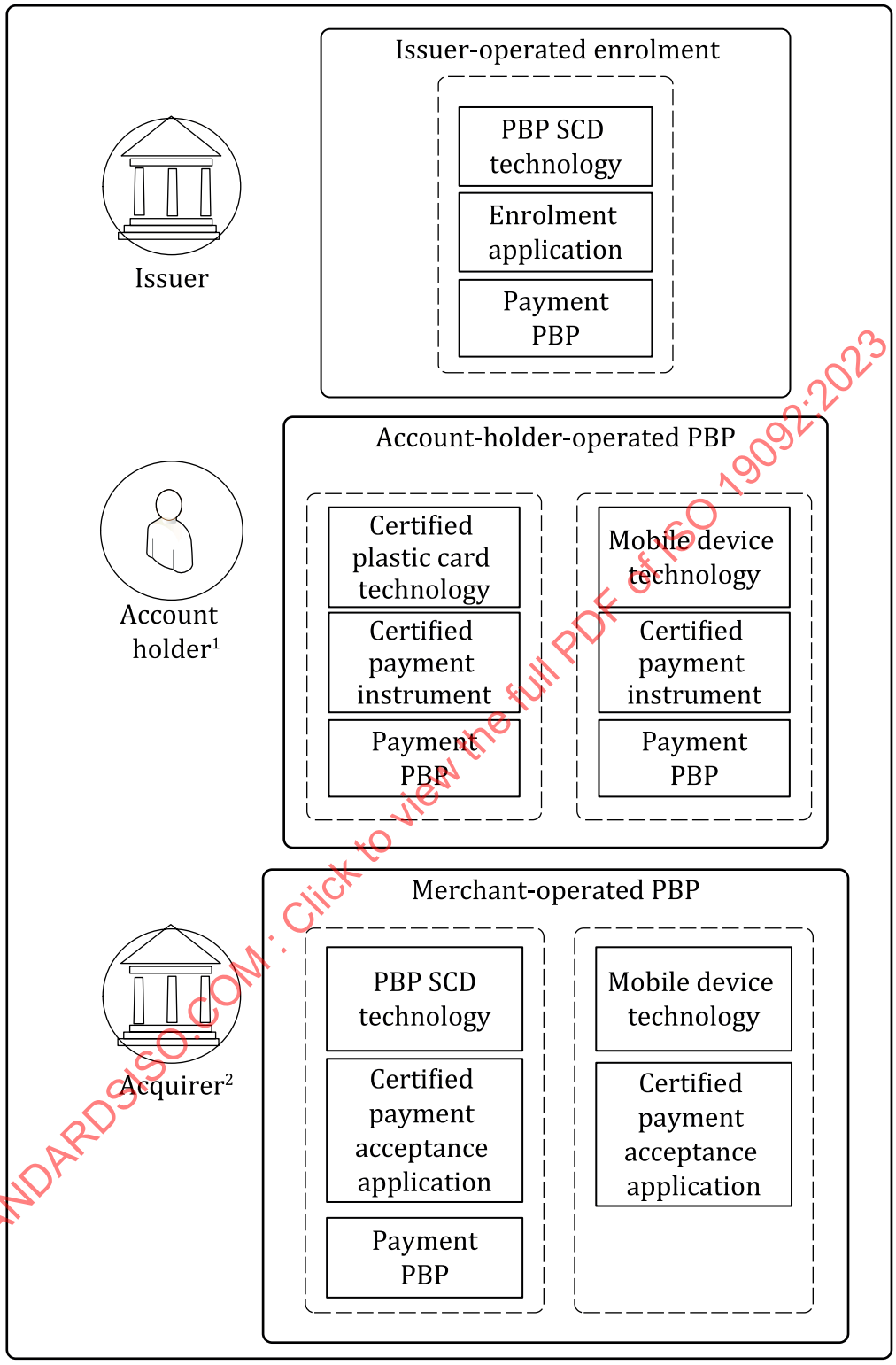
8.5.1 PBP device operators

The capture of authentication data is typically performed using devices operated by the issuer or the acquirer (or an entity the acquirer sponsors, e.g. a merchant). However, there is an option for the device to be operated by the account holder, as a device that is only used by that individual. This option was not heavily adopted for the capture of PINs, but it is prevalent in biometric authentication.

An account-holder-operated biometric capture device is a personal biometric capture device, as opposed to a public biometric capture device that is used by many people and operated by someone other than the account holder initiating the transaction. This differentiation is necessary when considering risks associated with a biometric authentication solution. PBP device operators are illustrated in Figure 8.

STANDARDSISO.COM : Click to view the full PDF of ISO 19092:2023

© ISO 2023 – All rights reserved



STANDARDSISO.COM : Click to view the full PDF of ISO 19092:2023

1 Cardholder device-access biometrics also allowed.

2 Merchant device-access biometrics also allowed.

Figure 8 — PBP device operators

© ISO 2023 – All rights reserved

8.5.2 PBP device types

The most common PBP device categories are as follows:

a) Public SCD PBP: a purpose-dedicated public payment device that is equivalent to an SCD-based PIN entry device, with the primary difference being in the use of biometric sensing in place of PIN entry. Such devices may also be used in the issuer domain (by the issuer or designated entity) for enrolment. See Annex B for additional information.

   For these devices, the comparison and decision-making logic is for security reasons unlikely to be located in the capture device.

b) PBP card: a personal smart card payment instrument with biometric sensing capability and commonly on-card biometric processing and reference storage functionality. These commonly support both biometric enrolment and transaction-authentication functions and include comparison and decision subsystems.

c) Personal MPBP: assumed to be a personal mobile phone or similar non-SCD device used as a payment instrument and providing biometric capture and processing functions. These can also be used for both biometric enrolment and transaction authentication.

   For these devices, the comparison and decision-making logic is most likely to be on the device.

d) Public MPBP: a personal mobile phone or similar non-SCD device used as a public merchant terminal with biometric capture and processing functions provided via an attached SBR.

8.5.3 Point of biometric presentation (PBP)

8.5.3.1 Enrolment presentation

Since the biometric data that will be used for authentication cannot be assigned, the enrolment process involves its capture and processing to create the biometric reference on which authentication decisions will be made. This is the PBP for biometric enrolment, and the data are collected using a biometric capture device.

The establishment of the reference data is considered to occur in the issuer domain (by the issuer or designated entity), as it is between the account holder and the issuer.

Figure 9 depicts the enrolment process using PBP devices.

STANDARDSISO.COM : Click to view the full PDF of ISO 19092:2023

© ISO 2023 – All rights reserved

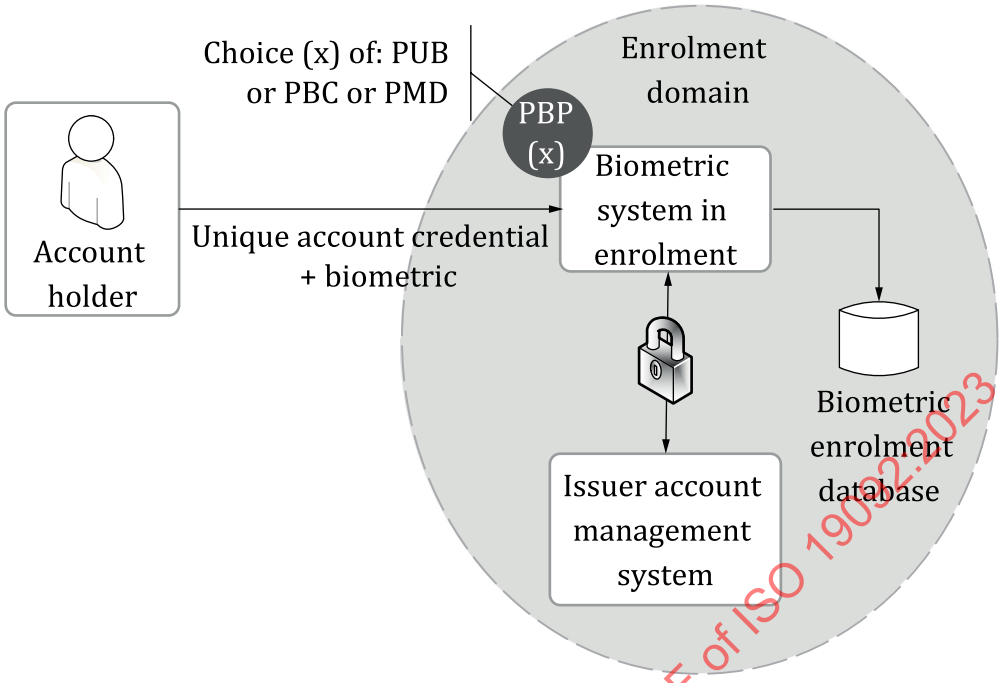


Figure 9 — Biometric enrolment using PBP devices

8.5.3.2 Payment transaction presentation

In both PIN and biometric authentication, the data are presented for comparison against the reference data.

When biometric data are used for authentication, the capture, feature extraction and verification can be performed using separate logical subsystems within the same physical device or some portion of the solution can include other devices or entities. A device where presentation and capture of the biometric data occurs is called the payment PBP. The biometric data are collected using the functionality of a biometric capture device. Such functionality may be incorporated in the PBP device or the solution may utilize a separate biometric capture device.

While both PIN and biometrics are captured for authentication, the processes for evaluations of the two devices types are different. The PIN is captured during the transaction by a class of devices known as SCDs. For such devices, there exists a formal program that:

— establishes device security requirements (including periodic review and update);

— sets criteria for measurement against those requirements;

— identifies testing laboratories that have been approved to evaluate the devices;

— provides a list of devices found by the laboratories to have been conforming to the requirements.

From that listing it is possible to identify the specific set of requirements on which a device type was measured and when the approval will expire, and to obtain a security document authored by the manufacturer of the device.

For biometric capture devices, there is no such program in place in the industry today. Security evaluation of biometric devices should employ methods consistent with evaluation of PIN entry devices but extending to those features specific to biometrics.

STANDARDSISO.COM : Click to view the full PDF of ISO 19092:2023

© ISO 2023 – All rights reserved

8.5.4 Biometric authentication architecture

8.5.4.1 SCD PBP device-based biometric authentication architecture

Public SCD PBPs include, at a minimum, the biometric capture interface, which in many implementations will embody biometric sample processing capability and presentation attack detection mechanisms. Such devices will support secure communications interfaces connecting them to the rest of the system infrastructure. Enrolment scenarios are described in Annex B.

One example of a possible flow using a public SCD PBP during a transaction is illustrated in Figure 10.

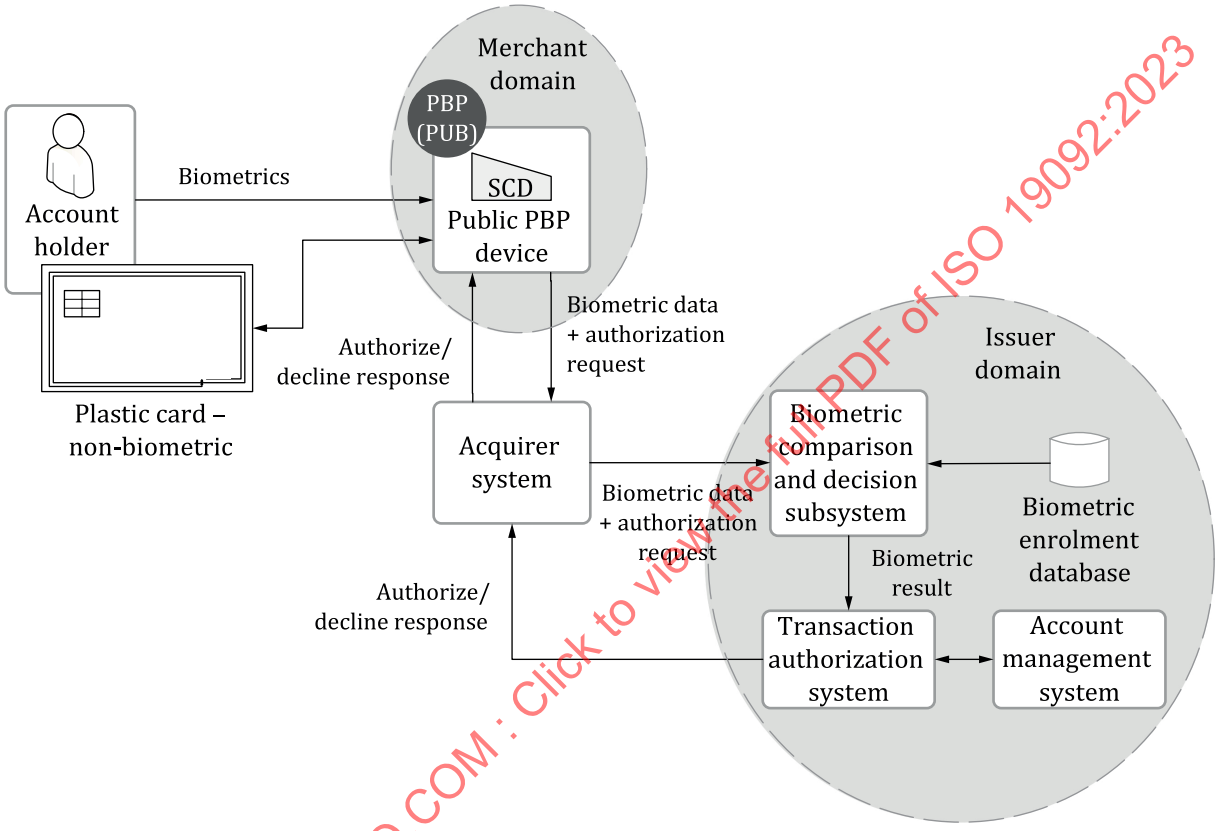


Figure 10 — SCD PBP in a transaction

8.5.4.2 PBP card-based biometric authentication architecture

8.5.4.2.1 General

Some biometric functions, such as biometric data capture, storage, feature extraction and comparison, are handled by the biometric card. The biometric card is defined in ISO/IEC 24787. ISO/IEC 24787 covers the three cases "off-card biometric comparison", "on-card biometric comparison" and "biometric-system-on-card". This document covers the two cases "on-card biometric comparison" and "biometric-system-on-card". Associated card data capture can be via the card's interface.

8.5.4.2.2 On-card biometric comparison

The comparison takes place on-card. "On-card biometric comparison" is illustrated in Figure 11. Biometric reference may be implemented in the issuer domain.

STANDARDSISO.COM : Click to view the full PDF of ISO 19092:2023

© ISO 2023 – All rights reserved

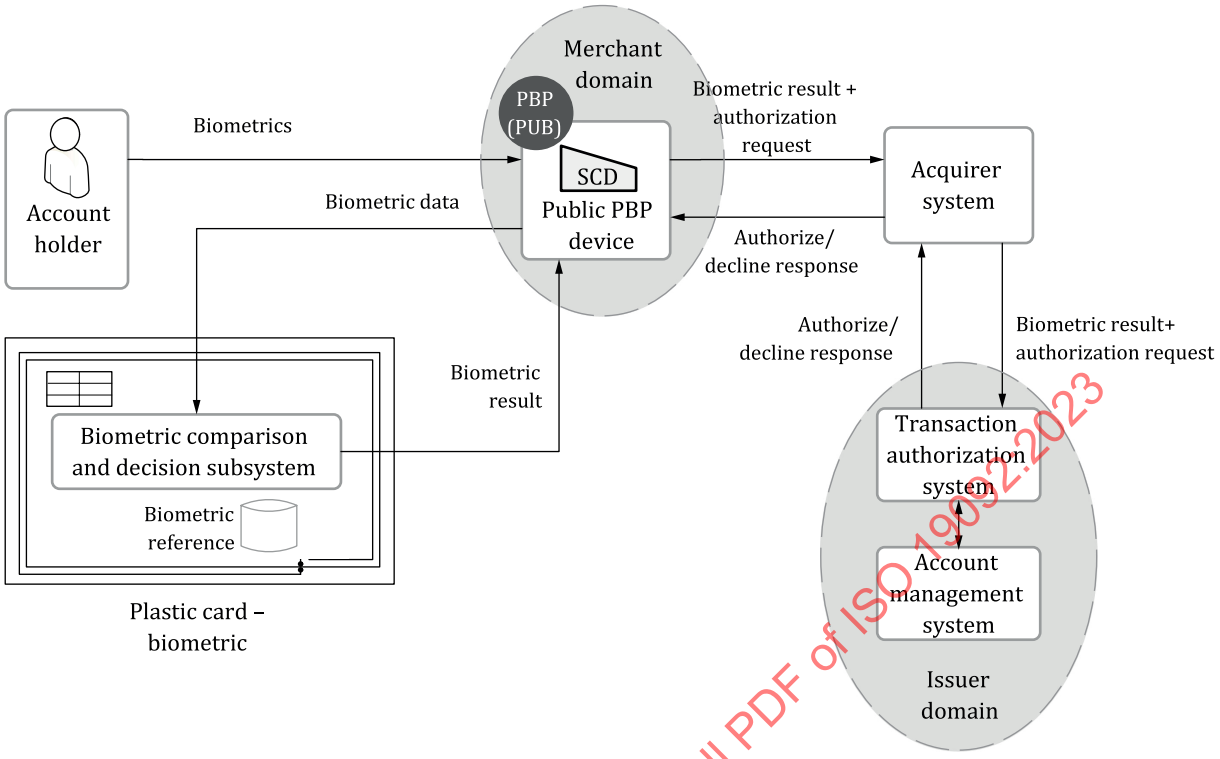


Figure 11 — on-card biometric comparison

8.5.4.2.3 Biometric system-on-card

Biometric system-on-card means that the whole biometric verification process is performed on a card, as illustrated in Figure 12.

STANDARDSISO.COM : Click to view the full PDF of ISO 19092:2023

© ISO 2023 – All rights reserved

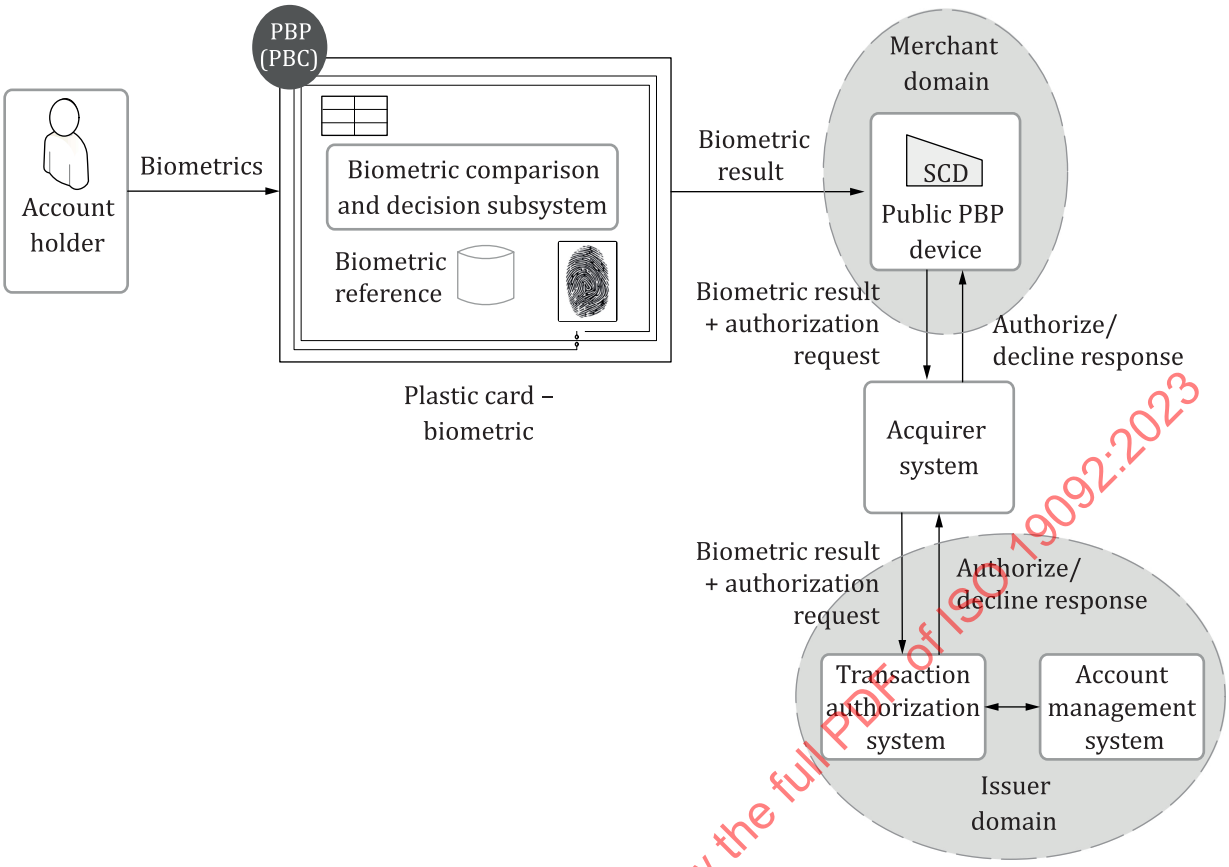


Figure 12 — Biometric system-on-card

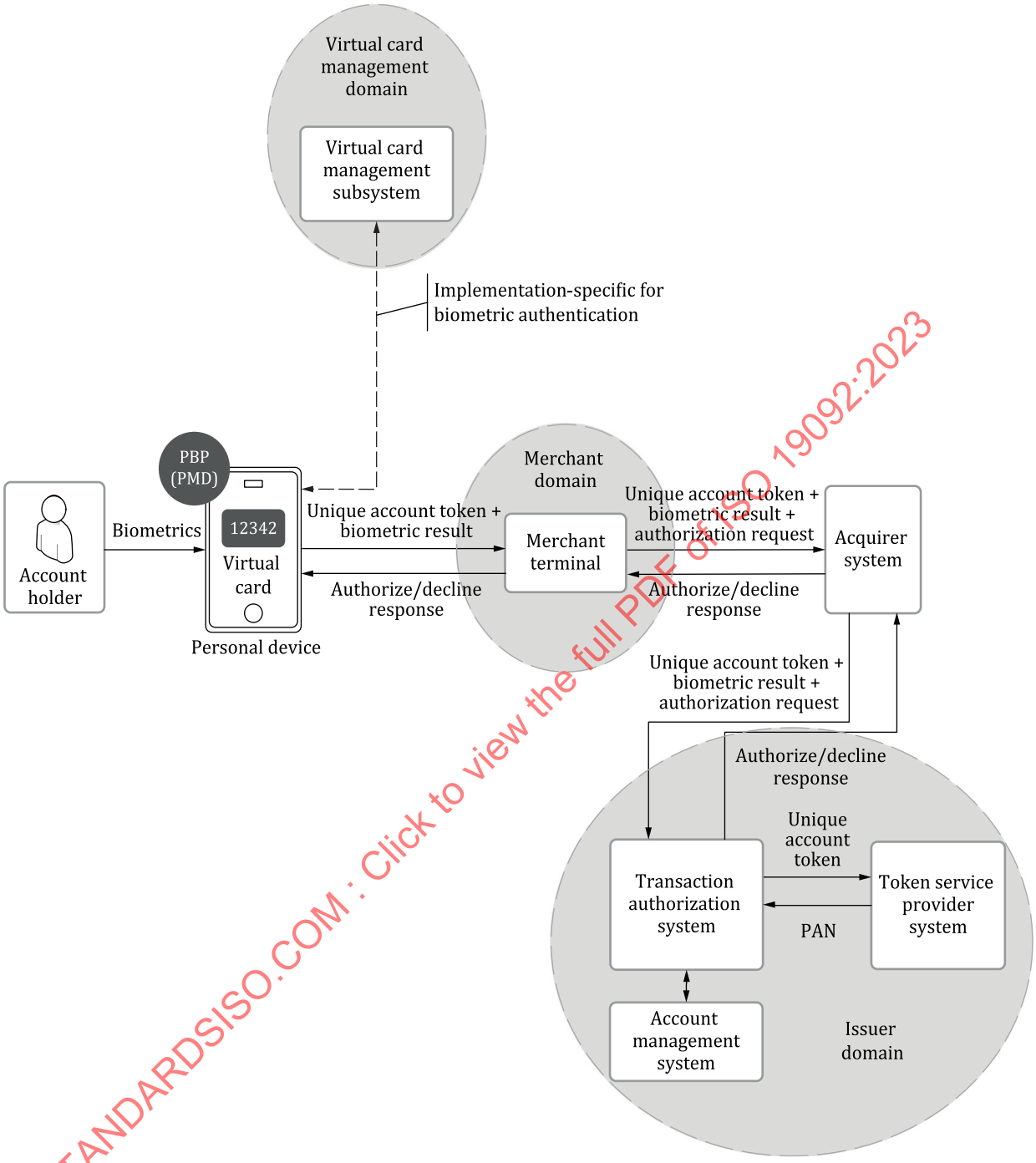
STANDARDSISO.COM : Click to view the full PDF of ISO 19092:2023

8.5.4.3 Mobile as a payment instrument-based biometric authentication architecture

Personal devices such as mobile phones are increasingly used as virtual payment instruments, normally in association with a wallet application. Such devices provide, at a minimum, the biometric capture interface and in typical implementations will also embody biometric reference storage, biometric feature extraction, presentation attack detection mechanisms and the comparison and decision-making mechanisms. Such devices should support secure communications interfaces, connecting them to the rest of the system infrastructure.

Figure 13 gives an illustration of a possible flow for a transaction using a mobile device as a payment instrument. Other flows are possible.

© ISO 2023 – All rights reserved



STANDARDSISO.COM : Click to view the full PDF of ISO 19092:2023

Figure 13 — Mobile device as a payment instrument in a transaction

8.5.4.4 Mobile as a payment terminal-based biometric authentication architecture

A merchant's personal mobile phone or other mobile device can be used in a public merchant terminal role in conjunction with an attached or integrated SBR. For more details about needing to achieve equivalent security to an SCD of the SBR, refer to 8.5.3.2. In this case biometric functions are handled by the SBR and communications with acquirer or issuer systems can be handled by either mobile devices or the SBR. Associated card data can be read via the device's contactless interface or via an additional interface on the SCR.

© ISO 2023 – All rights reserved

Transaction usage for this device category is similar to that of public SCD PBP devices, with the exception that the MPBP device can be used as the card reader if the biometric capture device does not provide this capability.

Figure 14 gives an illustration of a possible flow for a transaction using a mobile device as a merchant terminal. Other flows are possible.

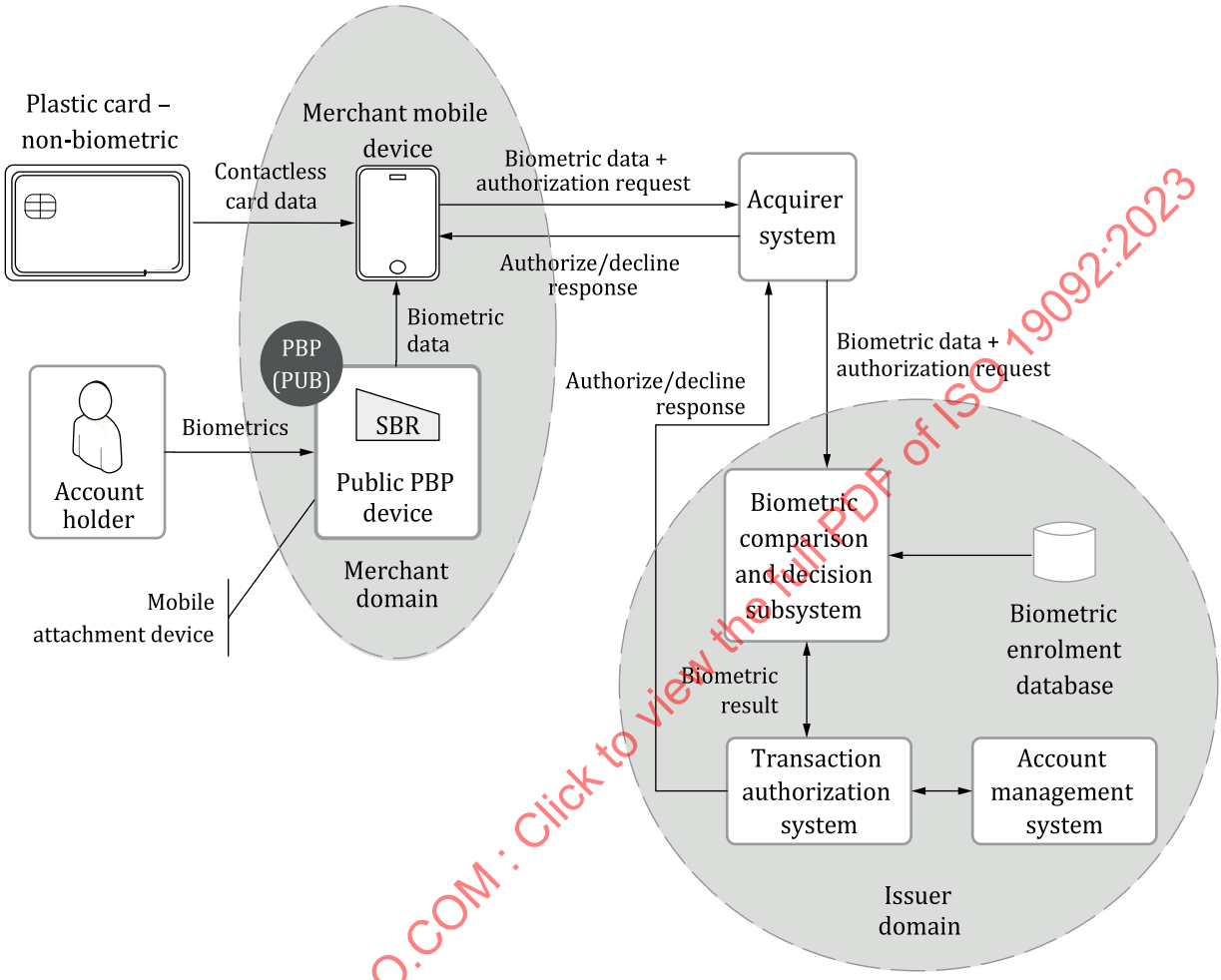


Figure 14 — Mobile device as a payment terminal in a transaction

STANDARDSISO.COM : Click to view the full PDF of ISO 19092:2023

9 Financial biometric authentication systems – threats and vulnerabilities

9.1 Generic threat considerations

As with traditional financial authentication systems, biometric systems are assumed to be under constant threat from fraud or mal intent, and to be susceptible to many similar vulnerabilities. Generic attack modalities and controls for retail financial systems are well known and controls for these are described in other International Standards.

Generic attacks against retail financial systems seek to exploit weaknesses in:

— physical and logical elements of data entry, data processing and storage subsystems;

— communications links between subsystems;

— cryptographic and procedural control design and implementation;

— key management design and implementation;

© ISO 2023 – All rights reserved

— application and POI technology design and implementation;

— user and administrative interfaces;

— payment system infrastructure access controls;

— equipment and software supply chains;

— security evaluation and certification regimes.

This document focuses mainly on security vulnerabilities which are unique to financial biometric authentication. Specific vulnerabilities considered in this document – within the context of the architectures described in Clause 8 – include the following:

a) public and personal PBP hardware and software vulnerabilities;

b) vulnerabilities in personal device on-platform and off-platform application provisioning subsystems;

c) vulnerabilities in personal device off-platform security management subsystems, including key management, security attestation and transaction delivery subsystems;

d) public and personal PBP sensor technology vulnerabilities;

e) biometric computational vulnerabilities relating to signal capture and feature extraction algorithms and mechanisms;

f) biometric computational vulnerabilities relating to biometric comparison and decision-making mechanisms;

g) vulnerabilities arising from automated biometric reference refinement mechanisms and the potential need to store more than one reference against a given identity;

h) protocol vulnerabilities arising from biometric subsystem interactions;

i) vulnerabilities arising in third-party biometric service domains and their interconnection to traditional payment systems infrastructure.

Reference is also made to

— potential vulnerabilities arising in biometric security evaluation regimes;

— potential vulnerabilities arising in personal device supply chains.

The following subclauses list vulnerabilities relating to biometric presentation (9.2) and comparison, decision and storage (9.3). See Annex A for threats and vulnerabilities for biometric environment.

9.2 Biometric presentation vulnerabilities

9.2.1 Overview

This subclause describes possible attacks against a PBP.

9.2.2 Synthetic biometric presentation attack vulnerabilities

A synthetic (artificially constructed) presentation attack is where an attacker fabricates an analogue of a legitimate user's biometric characteristics using captured information. That analogue is subsequently used to impersonate the user to the biometric system.

Some biometrics are susceptible to illicit capture in the presentation environment or elsewhere for possible use in developing a presentation attack. For example, video surveillance systems and pervasive camera technologies provide ample opportunities for certain modalities, such as face recognition or

STANDARDSISO.COM : Click to view the full PDF of ISO 19092:2023

© ISO 2023 – All rights reserved

even fingerprint recognition, when used in a biometric presentation environment. Likewise, postings on social media provide opportunities for face synthesis for attack purposes. Other modalities also provide side-channel opportunities, for example through the lifting of fingerprints from surfaces touched by a target identity. Such traces are typically ubiquitous.

A synthetic attack might involve the following steps:

— collection of biometric information representing one or more subject biometric sample; various methods exist for capturing the data necessary to build the presentation attack instrument;

— theft or capture from the individual (e.g. photograph face, capture fingerprint from water glass or severed finger);

— capture of raw biometric data or biometric reference from the biometric system (e.g. wiretaps, access to database);

— installation of fake biometric readers that users believe are part of the real system and collection of the entire biometric sample data entered through those readers;

— use of the collected biometric information to fabricate a physical analogue of the biometric sample and use of that against a PBP.

Potential controls include:

— robust presentation attack detection by the PBP technology;

— attended monitoring during biometric presentation.

— sufficient liveness detection to determine a living individual is behind the biometric sample (e.g. a vein-mapping sensor that will not verify a severed finger or hand).

NOTE ISO/IEC 30107 discusses artificial presentation attacks.

9.2.3 Improper PBP device calibration vulnerabilities

A legitimate operator may compromise or damage a biometric device during routine maintenance or installation. Likewise, an adversary might physically access the biometric device and modify the device's configuration. Either situation could lead to a comprise of biometric device operation.

The exact nature of such an attack against a PBP will be implementation-dependent.

9.2.4 Fault injection

As with other types of security equipment, hardware or software faults can be induced through various means, including power supply manipulation or process interruption at a critical phase. Trusted hardware capabilities should be used on a given platform.

9.3 Comparison, decision and storage subsystem vulnerabilities

9.3.1 Overview

The attacks described in this subclause are against the logic of the biometric comparison and decision-making processes.

For the comparison process, the biometric sample is compared with an enrolled biometric reference to create either a Boolean pass or fail output or a score.

The decision process involves applying policy settings to the output of the comparison process, possibly also taking into account historical or other parameters associated with the authentication process and concluding with a decision that the user has been authenticated or not for the forthcoming interactions or transaction.

STANDARDSISO.COM : Click to view the full PDF of ISO 19092:2023

© ISO 2023 – All rights reserved

When a submitted biometric sample and a biometric reference are compared, the resulting score can be said to represent a match if it exceeds a particular threshold and a non-match if it does not. A simple system decision policy that might be used in verification applications would be to accept the user's claim to an identity if a match occurs and reject the claim if a non-match is determined.

However, operational biometric systems typically use more sophisticated decision policies than this. For example, a verification system may allow a user at least three attempts to produce a score exceeding the match threshold. Consequently, for verification systems the effective acceptance and rejection rates are derived from the interplay between raw match or rejection rates and decision policy.

The relationship between FMR and FNMR is inversely proportional, due to the overlap between valid and invalid matches. The better the biometric system, the lower the value of both FMR and FNMR.

Match statistics for legitimate biometric users form a bimodal distribution between FMR and FNMR. Thresholds can be set to lower FNMR but increase FMR.

In conclusion, biometric threshold setting policy and decision policy can have a significant bearing on authentication security.

9.3.2 Improper threshold settings vulnerability

An improperly adjusted FMR or FNMR can result in an unauthorized individual gaining access or an authorized individual being denied access.

9.3.3 Score and threshold vulnerabilities

An attacker could utilize the results of a match to gain information to compromise the system systematically.

The exposure of scores emanating from biometric systems can present attack opportunities. For example, where an attacker can observe the comparison and decision process for a synthetic biometric under their control, perturbing presentation in a systematic way could allow the attacker to adjust the synthetic biometric until it meets system acceptance criteria. This is commonly referred to as a hill-climbing attack.

See Reference [29] for further information.

9.3.4 Reference refinement vulnerabilities

Where a biometric authentication implementation allows refinement, biometric references can be automatically updated to improve match metrics. The process is normally initiated by the comparison or decision subsystems, with a modified reference replacing the previous instance.

The update process applies to matched biometrics only, normally according to the following decision process:

— If the score for a match exceeds an upper threshold, the system indicates that the sample data matches the biometric reference and nothing else is done.

— If the score for a match exceeds a lower threshold, but not the upper threshold, the system indicates that the biometric reference is updated in some way using the sample data.

When an update is performed, the possibility may exist to inject a sample of an unauthorized individual into the update function, causing the return of a compromised new biometric reference.

The refinement process may also be vulnerable to the hill-climbing attack discussed in 9.3.3.

STANDARDSISO.COM : Click to view the full PDF of ISO 19092:2023

© ISO 2023 – All rights reserved

9.3.5 Self-targeted match search vulnerabilities

An attacker might try to verify their own biometric characteristic against a large number of biometric references in the system database in an attempt to find a match to some other random party, ultimately gaining illicit access to the target's account.

9.3.6 Other-party targeted match search vulnerabilities

An attacker with access to an accurate representation of an unknown person's characteristics might use a presentation or injection attack to use the authentication system to discover the identity of the characteristic's owner.

9.3.7 Match collision vulnerabilities

An attacker with direct or indirect access to a reference database might search for a random match between individual identities and seek to exploit the match, perhaps by persuading one of the parties to access the account of the other party.

9.3.8 Authentication result transmission vulnerabilities

In a financial biometric authentication implementation, the subsystems carrying out comparison and decision may be located in domains which are remote from the issuer or other reliant systems. Security vulnerabilities may exist:

— in the communications path travelled by authentication result messages between decision-making and account access;

— in the encoding module where the result is encoded for transmission; for example, in the personal device scenarios the result and any accompanying data are likely to be tokenized in some form.

9.3.9 Biometric storage vulnerabilities

Biometric storage systems will typically have similar vulnerabilities to those for PIN-based authentication systems. Similar controls can be applied; however, the frequency and extent of access to the references in a live system may render this subsystem more vulnerable to attack or reduce the effectiveness of intrusion detection.

STANDARDSISO.COM : Click to view the full PDF of ISO 19092:2023

10 Financial biometric authentication systems — security requirements

10.1 General

The following subclauses present security requirements that shall be applied to financial biometric authentication systems. 10.15 describes the requirements for testing and evaluation against the security requirements in this document. The biometric security controls checklists in Annex C shall be used to assess generic security controls and biometric reference life cycle controls.

10.2 Generic security requirements

10.2.1 Physical security requirements

10.2.1.1 PBP

Biometric devices shall employ physical security mechanisms in order to restrict unauthorized physical access to the contents of the device and to deter unauthorized use or modification of the device (including substitution of the entire device) when installed.

© ISO 2023 – All rights reserved

All public PBP devices shall meet security requirements equivalent to those defined in ISO 13491-1 and ISO 13491-2, supplemented or amended as defined in this document. That is, for requirements where exact conformity is not achieved, compensating controls shall be in place.

Personal biometric smart cards shall meet security requirements equivalent to ISO/IEC 15408-3 EAL4+ (as applying to non-biometric bank-issued smart cards), supplemented or amended as described in this document.

If a personal biometric device is not a smart card and not an SCD – as is the most likely scenario – then at a minimum it shall utilize a trusted domain (TD) for at least partial protection of keys used to protect on-platform biometric processes and shall, wherever possible, instantiate biometric processing operations within the TD. For biometric processing operations on a personal device that cannot be protected by a personal device's TD, obfuscation and attestation methods shall be used.

10.2.1.2 Other biometric subsystems

Biometric subsystems other than PBP shall be designed with the same level of security as for financial PIN-based authentication systems.

Provisioning, attestation and monitoring services supporting mobile financial application security for biometric authentication are likely to employ purpose-specific, potentially unstandardized key management mechanisms and procedures, implemented using one or more HSMs. Attestation and monitoring controls used for mobile devices are controls aimed at providing detection of intrusion.

10.2.2 Logical security requirements

The generic logical security requirements applying to all applications and environments wherever biometric information is captured or used are as follows:

a) Approved cryptographic mechanisms shall be in place to maintain the authenticity, integrity and confidentiality of biometric information within each processing or storage subsystem.

b) Approved cryptographic mechanisms shall be used to maintain the authenticity, integrity and confidentiality of communication channels between subsystems.

Biometric data shall be encrypted when stored or sent over a public network to provide confidentiality. The encryption algorithm shall be one of those defined in the ISO/IEC 18033 series or ISO/IEC 19772.

When entity authentication algorithms are used, the algorithm shall be one of those defined in ISO/IEC 9798.

Integrity shall be protected with cryptographic methods (digital signature or MAC) when biometric data are stored or sent over a public network. When integrity is provided by a digital signature, the digital signature algorithm shall be one of those defined in the ISO/IEC 9796 series or the ISO/IEC 14888 series. When integrity is provided by a MAC, the MAC algorithm shall be one of those defined in the ISO/IEC 9797 series and validated in accordance with ISO 16609.

For public biometric capture devices, key management techniques shall be in conformity with ISO 11568. For personal biometric capture devices, key management techniques shall either:

— be in conformity with ISO 11568; or

— achieve security equivalent to ISO 11568.

HSM APIs used for provisioning, attestation and monitoring services supporting mobile financial application security for biometric authentication shall be evaluated as secure against both general and application-specific security vulnerabilities.

Countermeasures against data extraction and replay attacks shall exist to protect the biometric tag authentication information. Controls such as protection of communication channels, pathways between

STANDARDSISO.COM : Click to view the full PDF of ISO 19092:2023

© ISO 2023 – All rights reserved

internal sensors, prevention of feature extraction and using physical protection or dynamic data in protocol messages such as nonce, challenge or timestamp shall be used.

10.3 Identity registration

10.3.1 Overview

Customer registration may occur separately from biometric enrolment or may be performed at the beginning of the enrolment process.

10.3.2 Security requirements

Before enrolling for financial biometric authentication, each prospective enrolee shall have registered with an associated identity management system, typically during the establishment of a bank account. One central function of registration is to establish the identity of a prospective biometric enrolee by requiring the presentation of evidence of identity.

Different jurisdictions will have precise but potentially differing requirements for meeting the registration threshold. Depending upon the jurisdiction and implementation, evidence of identity can be in the form of a birth certificate, driver's license or passport. Other credentials may also be acceptable.

Where the registered identity is to be that of a business or some other non-natural-person, further proof of authority may be required of the prospective enrolee.

10.4 Presentation

10.4.1 Overview

Presentation occurs when enrolling or authenticating.

10.4.2 Security requirements

When biometrics is presented for authentication purposes, presentation attack detection mechanisms shall be in place.

Security controls for unattended PBPs shall include design features providing visual, physical and logical mechanisms aimed at providing tamper evidence and tamper responsiveness, coupled to a routine field inspection regime.

Additionally, to prevent improper PBP device calibration and fault injection, proper policy, controls and audit procedures shall be prepared and performed.

10.5 Data storage and handling

10.5.1 Overview

General controls apply to access management of the biometric references as well as to their use in the comparison and decision process. One effective supplemental control involves reference splitting, as set out in the following subclauses. If the biometric references are split, then even if part of the biometric reference is leaked the rest is protected from the attacker.

10.5.2 Reference splitting procedure

Biometric information risks may be mitigated to some extent in some contexts by reference splitting. Here, a biometric reference is split into parts to be stored at different locations, with each part needing to be recovered during the comparison process.

STANDARDSISO.COM : Click to view the full PDF of ISO 19092:2023

© ISO 2023 – All rights reserved

In one example (see Figure 15), an identified customer presents their biometric reference at a financial institution where it is split with one part retained by the issuer and the other part transmitted to a TTP.

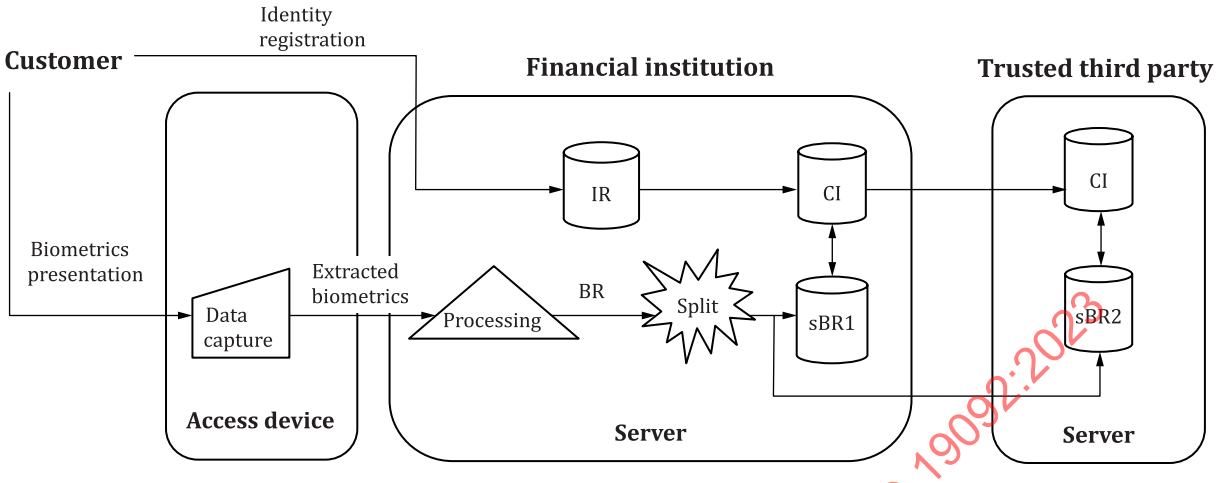


Figure 15 — Split reference enrolment

At authentication time (see Figure 16), the comparison subsystem recovers the split reference parts, recombines them to form the complete reference and uses that in the subsequent analysis.

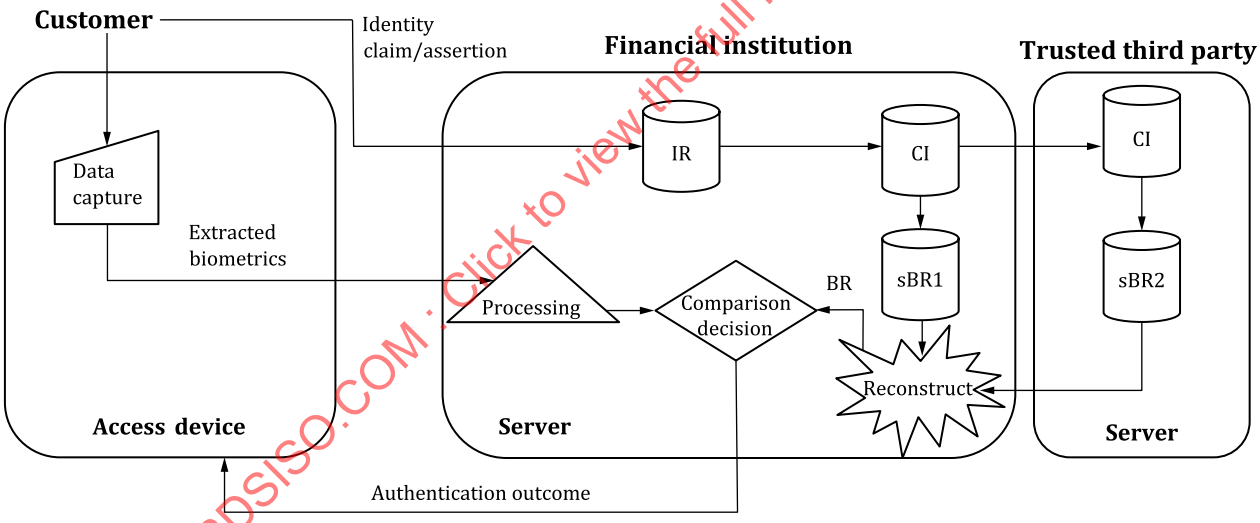


Figure 16 — Biometric authentication process

Use of reference splitting is optional, but if it is used the following security requirements shall apply:

a) The splitting process shall be such that it is infeasible to reconstruct a viable reference from one part alone.

b) The splitting process shall ensure that a stored part in any representation shall not match any other stored part, either for the same identity or any other identity, except by chance.

c) A reference shall only be held in its constructed state during enrolment, until split part storage is complete, after which the reference and any parts not committed to storage systems shall be immediately and irreversibly erased.

d) A reference shall only be held in its constructed state during authentication until a match or non-match decision has been made, after which the reference and any parts shall be immediately and irreversibly erased.

STANDARDSISO.COM : Click to view the full PDF of ISO 19092:2023

© ISO 2023 – All rights reserved

e) Compromise of one part does not provide any information about the reference that is split.

10.6 Comparison and decision

10.6.1 Overview

The biometric threshold setting and decision policy can have a significant influence on the authentication result and cause security threats.

10.6.2 Security requirements

Proper policy, controls and audit procedures shall be prepared and performed to prevent improper adjustment of the threshold value. To protect against the hill-climbing attack of systematically modifying the sample to obtain progressively higher scores until the decision threshold is met, the following security requirements apply:

a) The incremental value of comparison scores shall have sufficient step size, rather than continuous scores.

b) Authentication between the application program and the biometric system shall be in place to provide integrity.

10.7 Enrolment

10.7.1 Overview

Enrolment is the process through which an enrolee's identity and one or more biometric references are captured at enrolment time (see 10.7.2).

The binding mechanism ensures that the identity of a subject can be recovered using, or strongly correlated with, a presented biometric.

The binding mechanism and its inputs are discretionary to the identity or biometric service provider and might entail the use of cryptographic mechanisms.

NOTE The ISO/IEC 24760 series provides a framework for identity management.

10.7.2 Security requirements

In addition to the generic security requirements stated in 10.2, the following additional requirements for enrolment and re-enrolment apply:

a) Mechanisms and procedures shall be in place to ensure an enrolee is entitled to be enrolled.

b) Mechanisms and procedures shall be in place to verify the identity of the enrolee at enrolment time or before the activation of the enrolled biometrics.

c) Mechanisms and procedures shall be in place to ensure a biometric sample is of sufficient quality to be used as a biometric reference.

d) Mechanisms and procedures shall be in place to ensure only a valid biometric reference is captured from the enrolee at enrolment time.

e) Binding of biometric reference to the identity shall be protected against manipulation using approved cryptographic algorithms. Refer to ISO/IEC 24745.

f) Mechanisms and procedures shall be in place to ensure a morphed or stolen biometric sample is not accepted (see ISO/IEC 30107). For example, an independent authentication factor is required before the activation of the biometric authentication functionality. Live capturing is recommended to prevent face-morphing attacks.

STANDARDSISO.COM : Click to view the full PDF of ISO 19092:2023

© ISO 2023 – All rights reserved

To guarantee that the biometric profile has been accurately recorded and stored, a live match should be made of the applicant's biometrics to the newly stored biometric reference. For more information on biometric sample quality, see ISO/IEC 29794.

10.8 Re-enrolment

10.8.1 Overview

Re-enrolment is an enrolment activity for subsequent updates to the biometric reference beyond initial enrolment. It may entail:

— replacing the biometric reference (e.g. per a security policy addressing the biometric life cycle or because the previous reference did not work well for the user);

— changing biometric sources (e.g. using a different finger);

— changing biometric sensors (e.g. switching from finger image to iris scanning or moving from one fingerprint sensor to another fingerprint sensor).

10.8.2 Security requirements

The security requirements for re-enrolment are generally the same as for enrolment – including the applicability of the generic security requirements. The requirements for authenticating the enrolee may be satisfied by reusing information captured at the time of initial enrolment.

Termination of the previous biometric reference is required and archiving of the terminated biometrics may also be carried out as determined by system security policy.

10.9 Refinement

10.9.1 Overview

Biometric refinement refers to the process by which existing biometric references may be automatically adjusted to improve accuracy or reliability, including for characteristics which may vary gradually over time. This helps to protect against hill climbing or iterative replacement attacks.

A previously existing biometric reference might be adjusted to include information obtained at a more recent time instance. For example, minutiae points may be added to or deleted from the registered template of a fingerprint, based on information observed in recently acquired samples.

10.9.2 Security requirements

In addition to the generic security requirements in 10.2, the primary additional security requirement for biometric refinement is that the refinement mechanism should increase neither FMR nor FNMR. If the security implementation affects FMR or FNMR, its impact shall be evaluated.

10.10 Verification

10.10.1 Overview

In the biometric verification process, the required biometric characteristic presented by the user is compared with the user's biometric reference after initial processing.

The verification process consists of the raw biometric data being captured in the data capture subsystem, the sample biometric features being generated by the feature extraction subsystem, a specific biometric reference being retrieved from storage and the comparison of sample features to the biometric reference being made by the comparison subsystem. Comparison results are forwarded to a decision process.

STANDARDSISO.COM : Click to view the full PDF of ISO 19092:2023

© ISO 2023 – All rights reserved

Although biometric reference adaptation is performed in the comparison subsystem, the judgement as to whether or not to accept the adaptation and update an enrolled biometric reference in storage may also involve the decision subsystem.

Error rates differ among various biometrics. Due to the variable nature of physical characteristics and human behaviour, it is difficult to determine a universally consistent biometric error rate. The variables involved in determining an accurate error rate include issues relating to correct use of the biometrics, environmental conditions and user training or acceptance. This document assumes that the biometrics are presented under ideal conditions.

10.10.2 Security requirements

When evaluating overall system security, deployers should document biometric decision policy issues, including noting that there is a critical difference between the single-attempt FMR and FNMR and the effective FMR and FNMR. A system's effective FMR and FNMR are the rates calculated when all policy relaxations, such as multiple retries and threshold adjustments, have been applied to a representative sample of presentations.

For example, a system whose decision policy allows for multiple attempts against multiple enrolment biometric references for a given user will have a higher effective FMR than its single-attempt FMR.

For verification systems, the corresponding FNMR of the biometrics shall be consistent with requirements of biometric management policy.

10.11 Identification

10.11.1 Overview

The biometric identification process is used to recognize an individual from other individuals using a set of biometric references. Here, the user presents the required biometric characteristic and the system compares the post-conditioning biometric data to a set of biometric references held in the system database.

The identification process consists of the raw biometric data being captured and conditioned, the sample biometric features being extracted by signal processing, multiple biometric references being retrieved from storage and multiple biometric reference comparisons and decisions being made by comparison and decision subsystems.

In the simplest case, the system stops checking biometric references as soon as a match is found and returns the identity associated with that matched biometric reference to the calling process. Alternatively, the comparison is made against all prospective biometric references.

10.11.2 Security requirements

The security requirements for verification are also applied to identifications. Significantly lower FPIR and FNIR should be employed for systems that employ a single biometric for identification than systems that are used for verification. Determining the proper FPIR and FNIR is contingent on the number of identification attempts, the size of the database against which attempts are executed and the overall decision policy.

In order to ensure the highest possible system accuracy in an identification system (especially in the case of large databases), it may be necessary to utilize high-quality sensors (typically higher than needed for verification systems) to generate high-quality sample data. Higher threshold settings may also be necessary.

It is critical that the enrolment for identification be of sufficient quality to enable an accurate search. Low-quality enrolment is more likely to allow the individual to be registered in the system on multiple occasions.

STANDARDSISO.COM : Click to view the full PDF of ISO 19092:2023

© ISO 2023 – All rights reserved

10.12 Termination

10.12.1 Overview

Biometric termination is the process of expunging a user's biometric reference data or making that data obsolete. Termination may be triggered by a number of factors, including:

a) the user requests to be removed from the system;

b) the enrolment period for the user has expired (e.g. a smart card user whose card has reached its expiration date);

c) an associated account is inactivated or deleted;

d) a biometric technology upgrade;

e) the biometric characteristic has changed enough to warrant creation of a new reference;

f) the biometric reference data has been compromised;

g) detection of fraud;

h) legal or regulatory measures.

10.12.2 Security requirements

In addition to the generic security requirements in 10.2, the following security requirements apply to termination:

— Termination shall be carried out by authorized persons or an authorized automated process.

— The termination process shall ensure that all associated references for a given identity are terminated.

— Termination events shall be logged for possible future audit.

10.13 Suspension and reactivation

10.13.1 Overview

The possibility exists that the use of biometric data could be put "on hold" or "restricted" for a period. This would be analogous to a credit-card authorization being restricted for reasons such as fraudulent activity. Depending upon the outcome of an investigation, the biometric data could be "activated" again or be assigned a termination status.

Reactivation is the process of returning a biometric reference to active use from suspension.

The suspended or active state of a biometric reference might be stored as a flag along with the reference.

10.13.2 Security requirements

In addition to the generic security requirements in 10.2, the following security requirements apply to suspension and reactivation:

— Suspension and reactivation shall be carried out only by authorized persons or an authorized automated process.

— Suspension and reactivation processes shall ensure that all associated references for a given identity are suspended or reactivated at the same time and atomically.

— Suspension and reactivation events shall be logged for possible future audit.

STANDARDSISO.COM : Click to view the full PDF of ISO 19092:2023

© ISO 2023 – All rights reserved

10.14 Archiving

10.14.1 Overview

Biometric archiving is the process of securely storing biometric data for non-operational purposes.

10.14.2 Security requirements

In addition to the generic security requirements in 10.2, the following security requirements apply to archiving:

a) Access control mechanisms shall be in place to prevent unauthorized access to archived biometric data.

b) Measures shall be in place to prevent an archived biometric reference being restored to a system in which it has been terminated or to an active state when it has been deactivated.

c) Restoration from archives shall only be permitted for purposes of forensics.

d) Archiving and restoration events shall be recorded in a log for possible future audit.

10.15 Security compliance verification

Security compliance verification against this document shall include laboratory evaluations or security audits covering the following:

— the security qualities of biometric capture, feature extraction and comparison computational functions;

— the security of presentation environment, i.e. the path between a presented biometric and the biometric system's signal capture hardware and software elements;

— the physical and logical security of biometric capture and feature extraction hardware and software domains;

— the security of the environment in which biometric capture and feature extraction subsystems are located;

— the physical and logical security of biometric storage, comparison and decision subsystems;

— the security of communications paths between physical or logical security subsystems;

— the security of the binding process or mechanism associating a biometric reference and its associated identity elements;

— the security fitness of the associated identity management system;

NOTE For additional security compliance guidance, refer to ISO/IEC 19792.

— the existence of a biometric security management process.

The compliance of any authentication system in terms of its consistency and accuracy requirements may be ascertained by an audit trail in an event journal. Biometric authentication control objectives should be used in the compliance process.

Financial biometric authentication compliance shall be validated by an independent laboratory or other assessing expert body. Such bodies will typically issue a formal compliance attestation report that can be made public.

STANDARDSISO.COM : Click to view the full PDF of ISO 19092:2023

© ISO 2023 – All rights reserved

Annex A
(informative)

Threats and vulnerabilities for biometric environments

A.1 Card vulnerabilities and mitigations

The addition of biometric capture, processing or storage features to a smart card should be done in a manner that is consistent with payment industry security requirements for non-biometric payment cards.

Additional considerations are as follows:

— With the exception of biometric signal capture, all on-card biometric processing should be done in the secure element.

— The path between biometric signal capture components and secure element should be protected.

— Post-personalization physical or logical modification of on-card biometric signal capture components should not be possible without causing visible damage.

— Cryptographic security measures should be used to protect the interaction between the card secure element and off-card biometric components, including protection of match results.

A more detailed guide to on-card biometric comparison is provided in ISO/IEC TR 30117.

A.2 Mobile devices vulnerabilities and mitigations

A.2.1 Overview

Mobile devices are able to support biometric authentication for financial transactions. Mobile devices discussed in 8.5 present numerous security challenges compared with comparable SCD implementations. The following subclauses provide a selection of generic safeguards for deployment of biometric authentication on mobile devices.

A.2.2 Mobile device generic vulnerabilities

The following applies to most practical biometric authentication application scenarios, with limited exceptions:

— Mobile devices on which they are instantiated provide limited or no hardware-based tamper-responsive or tamper-resistant security capabilities for the protection of sensitive data, sensitive application code or interfaces to biometric sensors.

— Such hardware security features as may be available to the application will in most cases have limited key management functionality, able only to provide security services to limited aspects of the application.

— Application security will be highly dependent on features of the platform operating systems, drivers and access permissions management which are partly or largely opaque to security audit or unverified or unverifiable trust levels, of no attributable security accountability and which historically have been significantly exposed to attack vectors.

— Given the critical importance of presentation attack detection to the integrity of biometric authentication generally, the difficulty of implementing, of achieving adequate security assurance

STANDARDSISO.COM : Click to view the full PDF of ISO 19092:2023

© ISO 2023 – All rights reserved

levels or of assessing the same for such mechanisms on general-purpose mobile computing platforms presents significant challenges.

— By virtue of generic vulnerabilities of the underlying device platform environment, and due to its significant internet-actuated capability, applications will, depending on design, potentially be exposed to rapid attack escalation onto multiple devices.

— Application security will also be highly dependent on features of the initial and subsequent code and data element provisioning processes onto the mobile platform.

In the case of initial provisioning, applications will in most cases be instantiated onto the device in undifferentiated generic form via third-party application stores using processes and environments not subject to independent security audit or certification, of no attributable security accountability and using cryptographic techniques proprietary to the application store operator or operating system provider.

In the case of subsequent provisioning – in which the application is rendered uniquely distinguishable from all other instances of that application – the provisioning process potentially uses complex non-standardised messaging and cryptographic protocols built on top of the unverifiable trust layer established by initial provisioning. Such provisioning will almost certainly be given effect by back-end subsystems responsible for dynamic key and potentially code management for the application, as well as for the authentication data emanating from the device for consumption by later acquirer and issuer systems.

Such service entities all normally include application stores, but may also extend to:

— applications stores;

— cloud-based security and key-management service provision;

— third-party application manage provision, including unique provisioning and attestation services;

— tokenization services;

— transaction processing services.

Such software obfuscation and attestation measures as are likely to be used in an attempt to compensate for the absence of hardware anti-tamper measures on the device will, given the current state of practice and academic analysis, and in the absence of standardization, be of unverified and most probably questionable security strength.

Such software attestation – code, data or operational intrusion detection and reporting – measures as are likely to be used will themselves be vulnerable in a hard-to-assess way to the underlying security vulnerabilities of the device platform, will operate in a domain where no viable security standards exist and may rely on arbitrary metrics for trigging a response to a perceived intrusion.

Such software provisioning and attestation measures, in practical implementations, may involve third-party source code or data suppliers and potentially run-time involvement of such parties.

Application security may also have significant side-channel exposure to co-resident applications or low-level commercial monitoring activities by operating system suppliers or application store operators.

Depending on design, applications may also be vulnerable to relay attacks in which the mobile platform presented in the merchant PBP environment may simply, but with low probability of detection, be used as conduit to an illicit remote biometric presentation.

For more information about security for mobile financial services, refer to ISO/TS 12812-2.

STANDARDSISO.COM : Click to view the full PDF of ISO 19092:2023

© ISO 2023 – All rights reserved

A.2.3 Controls for using an SBR with a mobile device

When a mobile device (typically a merchant device) is used with an SBR attachment, the following controls should be considered:

— secure management of the SBR in accordance with its security policy;

— provision of unique cryptographic binding between mobile application and SBR;

— use of secure transport and application-layer disciplines (authentication and encryption) between mobile application and SBR;

— use of secure transport and application-layer disciplines (authentication and encryption) between SBR and acquirer or other back-end interface for the transfer of biometric data or match results.

STANDARDSISO.COM : Click to view the full PDF of ISO 19092:2023

© ISO 2023 – All rights reserved

Annex B
(informative)

Biometric implementation scenarios

B.1 Overview

This clause describes concrete implementation scenarios for the differing PBPs described in Clause 8. The following descriptions are not exhaustive of all possible or permitted architectural scenarios. Rather, the following scenarios represent a realistic implementation.

B.2 On-card PBP

B.2.1 General

Biometric smart cards are typically issued by a financial institution and used as payment instruments with integrated biometric capability.

Biometric card hardware and software will, at a minimum, instantiate the capture interface.

For most practical implementations the card chip will also embody biometric reference storage, sample processing capability, presentation attack detection mechanisms and the comparison and decision-making mechanisms. The card will support a secure communications interface connecting it to the payment terminal to which the card is presented and, in online mode, to the issuer via acquirer infrastructure.

Due to the small footprint of a biometric card, its presentation attack detection or other biometric functionality will be significantly constrained.

NOTE Hybrid systems where biometric processing is shared between card and secure (SCD-grade) terminal or other secure system nodes are not precluded.

B.2.2 Enrolment-time scenario

The exact technical approach for enrolment for biometric cards will be defined by the issuer and is out of scope for this document; however, one possible enrolment architecture is illustrated in Figure B.1. Here, the card is supplied with a small battery-powered sleeve which provides power to the card and may, via an on-sleeve microcontroller, control some facet of the enrolment process, although not handling biometric data itself. The sleeve might carry a unique passcode initialised to it by the issuer or some similar authentication credential needing to be verified by the card prior to enrolment.

STANDARDSISO.COM : Click to view the full PDF of ISO 19092:2023

© ISO 2023 – All rights reserved

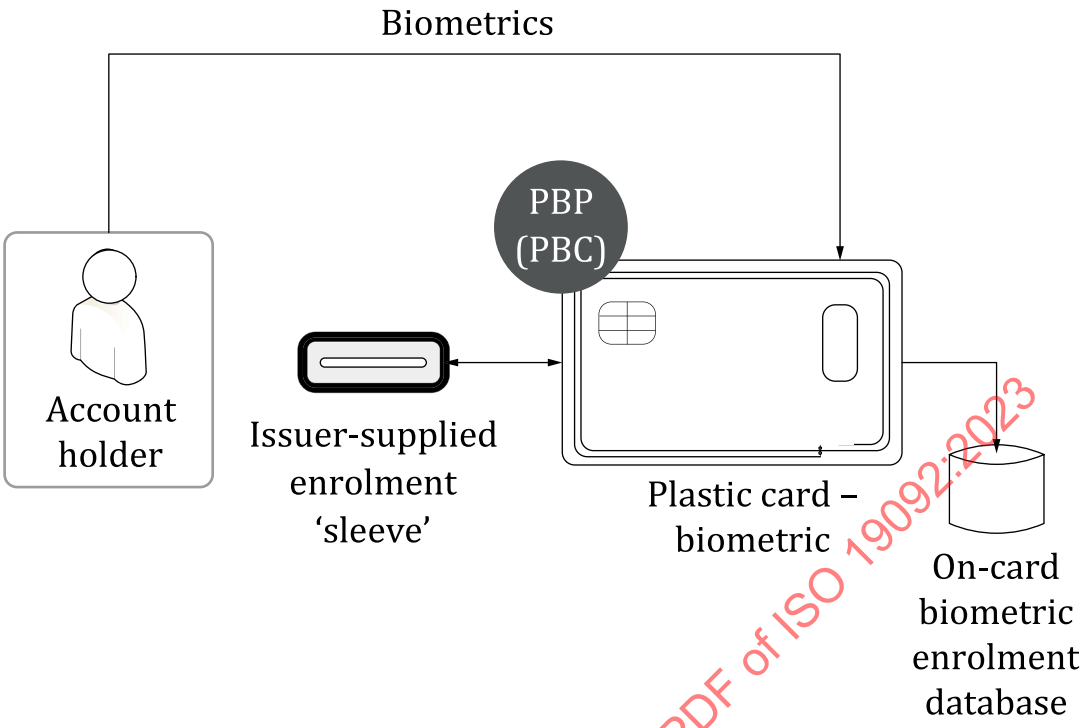


Figure B.1 — Card-based biometric enrolment with 'sleeve'

Alternative enrolment architectures might include those illustrated in Figure B.2 using a secure public device or a personal card reader attached to a personal computer, with passcode activation of the enrolment process.

Other architectures are also possible.

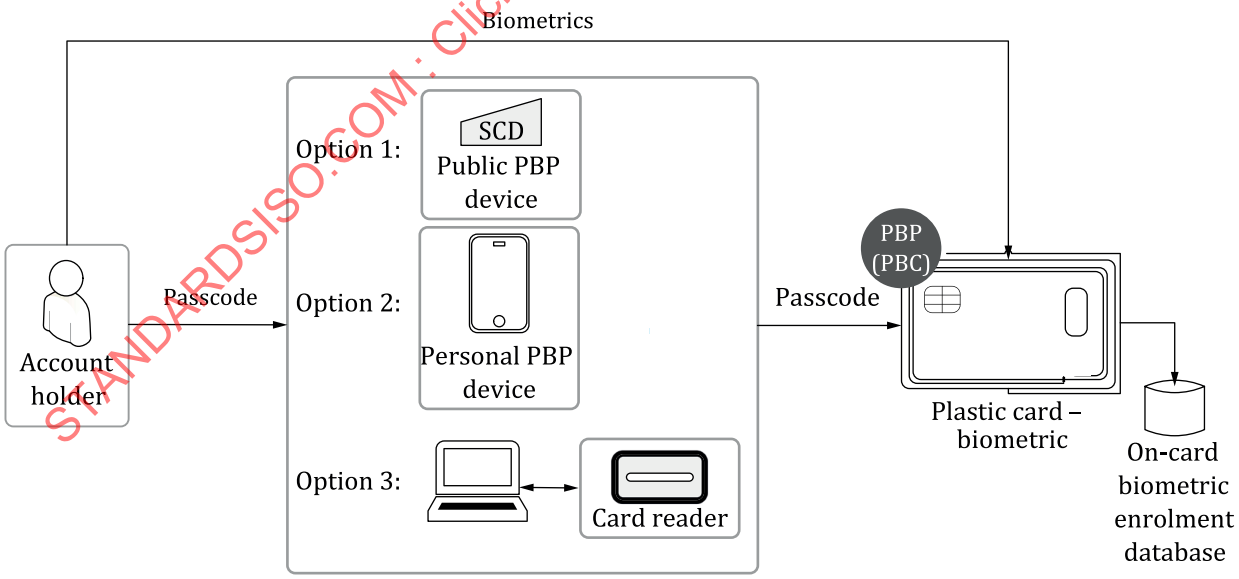


Figure B.2 — Card-based biometric enrolment with various other interface devices

B.2.3 Transaction-time scenario

A representative transaction-time architecture for a biometric card PBP is illustrated in Figure B.3.

STANDARDSISO.COM : Click to view the full PDF of ISO 19092:2023

© ISO 2023 – All rights reserved