



BSI Standards Publication

Financial services — Biometrics — Security framework

National foreword

This British Standard is the UK implementation of [ISO 19092:2023](#).

The UK participation in its preparation was entrusted to Technical Committee IST/12, Financial services.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

© The British Standards Institution 2023
Published by BSI Standards Limited 2023

ISBN 978 0 539 06166 6

ICS 03.060; 35.240.40

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 April 2023.

Amendments/corrigenda issued since publication

Date	Text affected
------	---------------

INTERNATIONAL STANDARD

ISO
19092

Second edition
2023-03-02

Financial services — Biometrics — Security framework

Services financiers — Biométrie — Cadre de sécurité



Reference number
ISO 19092:2023(E)
Documents
Document Sharing Hub
© ISO 2023



COPYRIGHT PROTECTED DOCUMENT

© ISO 2023, Published in Switzerland

All rights reserved. Unless otherwise specified, 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
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

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

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

Bibliography	63
---------------------------	-----------

Foreword

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

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

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

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

The main changes are as follows:

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

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

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

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

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

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

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

This page deliberately left blank

Financial services — Biometrics — Security framework

1 Scope

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

The following are within the scope of this document:

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

The following are not within the scope of this document:

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

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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

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

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

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

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

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

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

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

[ISO/IEC 19772](#), *Information security — Authenticated encryption*

3 Terms and definitions

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

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at <https://www.iso.org/obp>
- IEC Electropedia: available at <https://www.electropedia.org/>

3.1 biometric authentication

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

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

3.2 biometric capture

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

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

3.3 biometric capture device

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

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

3.4 biometric data

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

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

3.5 biometric enrolment

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

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

3.6 biometric enrolment database

database of biometric enrolment data record(s)

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

3.7

biometric feature extraction

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

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

3.8

biometric identification

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

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

3.9

biometric information

information conveyed or represented by biometric data

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

3.10

biometric policy

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

3.11

biometric presentation

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

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

3.12

biometric reference

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

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

3.13

biometric reference adaptation

automatic incremental updating of a biometric reference

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

3.14

biometric sample

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

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

3.15

biometric system

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

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

3.16

biometric system-on-card

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

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

3.17

biometric verification

process of confirming a biometric claim through comparison

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

3.18

biometrics

automated recognition of individuals based on their biological and behavioural characteristics

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

3.19

claimant

individual making a claim that can be authenticated in biometric authentication

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

3.20

comparison

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

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

3.21

comparison score

score

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

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

3.22

confidentiality

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

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

3.23

credential

representation of an identity for use in authentication

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

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

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

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

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

3.24

decision policy

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

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

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

3.25

encryption

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

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

3.26

false match rate

FMR

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

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

Note 2 to entry: Comparisons between:

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

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

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

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

3.27

false-negative identification rate

FNIR

FNIR (N, R, T)

proportion of a specified set of identification transactions by capture subjects enrolled in the system for which the subject’s correct reference identifier is not among those returned

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

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

3.28

false non-match rate

FNMR

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

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

3.29

false-positive identification rate

FPIR

FPIR (N , T)

proportion of identification transactions by capture subjects not enrolled in the system for which a reference identifier is returned

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

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

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

3.30

initial enrolment

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

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

3.31

integrated circuit card

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

3.32

integrity

property of accuracy and completeness

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

3.33

on-card biometric comparison

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

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

3.34

payment token

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

3.35

point of biometric presentation

PBP

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

3.36

presentation attack

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

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

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

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

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

3.37

presentation attack detection

automated determination of a presentation attack

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

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

3.38

re-enrolment

process of establishing a new biometric reference replacing existing biometric data for a subject already enrolled

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

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

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

3.39

registration

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

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

3.40

secure biometric reader

SBR

secure cryptographic device embodying biometric capture device and associated biometric processing software

3.41

secure cryptographic device

SCD

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

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

3.42

secure element

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

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:

- 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.
- 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.
- 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.

- 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.

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.

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 similar points.

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

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.