

INTERNATIONAL STANDARD

ISO
19092-1

First edition
2006-12-01

Financial services — Biometrics — **Part 1:** **Security framework**

Services financiers — Biométrie —
Partie 1: Cadre de sécurité



Reference number
ISO 19092-1:2006(E)



Documents
Document Sharing Hub
© ISO 2006

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

© ISO 2006

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword.....	v
Introduction	vi
1 Scope	1
2 Conformance	2
3 Normative references	2
4 Terms and definitions.....	2
5 Symbols and abbreviated terms	8
6 Biometric technology overview.....	9
6.1 Introduction	9
6.2 Fingerprint biometrics	9
6.3 Voice biometrics	10
6.4 Iris biometrics	10
6.5 Retina biometrics	11
6.6 Face biometrics.....	11
6.7 Hand geometry biometrics	11
6.8 Signature biometrics	12
6.9 Vein biometrics	12
7 Technological considerations	12
7.1 Biometric system properties	12
7.2 Universality.....	13
7.3 Distinctiveness.....	13
7.4 Accuracy.....	13
7.5 Performance evaluation	15
7.6 Interoperability	17
8 Basic principles of biometric architectures	17
8.1 Biometric system model	17
8.2 Data collection subsystem	18
8.3 Transmission subsystem.....	18
8.4 Signal processing subsystem	18
8.5 Matching subsystem	19
8.6 Decision subsystem	20
8.7 Storage subsystem.....	20
8.8 Portable tokens	20
9 Management and security requirements.....	21
9.1 Basic applications	21
9.2 Core security requirements	21
9.3 Enrolment	22
9.4 Verification	24
9.5 Identification.....	24
9.6 Transmission and storage	25
9.7 Termination and archiving	26
9.8 Compliance and event journal.....	27
10 Security infrastructure	27
10.1 Components	27
10.2 Physical techniques	29
11 Biometric validation control objectives.....	30

11.1	Periodic review and audit considerations	30
11.2	Environmental controls	31
11.3	Key management life-cycle controls	43
11.4	Biometric information life cycle.....	48
Annex A	(informative) Event journal.....	58
Annex B	(normative) Biometric enrolment	62
Annex C	(normative) Security considerations	64
Annex D	(normative) Security requirements for biometric devices	76
Annex E	(informative) Existing applications.....	79
Bibliography		81

Foreword

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

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

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

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO 19092-1 was prepared by Technical Committee ISO/TC 68, *Financial services*, Subcommittee SC 2, *Security management and general banking operations*.

ISO 19092 consists of the following parts, under the general title *Financial services — Biometrics*:

— *Part 1: Security framework*

The following parts are under preparation:

— *Part 2: Message syntax and cryptographic requirements*

Introduction

Business practice has changed with the introduction of computer-based technologies. The substitution of electronic transactions for their paper-based predecessors has reduced costs and improved efficiency. Trillions of dollars in funds and securities are transferred daily on systemically important payment systems and other financial systems by telephone, wire services and other electronic communication mechanisms. The high value or sheer volume of such transactions within an open environment exposes the financial community and its customers to potentially severe risks from accidental or deliberate alteration, substitution or destruction of data. Interconnected networks, and the increased number and sophistication of malicious adversaries compound this risk.

The inevitable advent of electronic communications across uncontrolled public networks, such as the Internet, is also increasing risk to the financial industry. The necessity to expand business operations into these environments has elevated the awareness for strong authentication and created the need for alternate forms of authentication. The financial community is responding to these needs.

Biometrics, the “something you are or are able to do” identity factor, has come of age, and includes for example such technologies as finger image, voice identification, eye scan, facial image. The cost of biometric technology has been decreasing while the reliability has been increasing, and both are now acceptable and viable for the financial industry.

This part of ISO 19092 describes adequate controls and proper procedures for using biometrics as an authentication mechanism for secure remote electronic access or local physical access controls for the financial industry. ISO 19092-2 describes the techniques, protocols, cryptographic requirements and syntax for using biometrics as an identification and verification mechanism in a wide variety of security applications in the financial industry.

Biometrics can be used for human authentication for physical and logical access. Logical access can include access to applications, services or entitlements. ISO 19092 promotes the integration of biometrics into the financial industry, and the management of biometric information as part of the overall information security management programme of the organization. It positions biometric technology to strengthen public key infrastructure (PKI) for higher authentication, by providing stronger methods as well as multi-factor authentication. In addition, this part of ISO 19092 allows continuous reassurance that the entity about to generate a digital signature is, in fact, the person authorized to access the private key.

The success of a biometric system with the public is based on a number of factors, and these factors differ among the available biometric technologies:

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

The authentication systems discussed in ISO 19092 are those for closed user groups, in which the group members have agreed to use biometric identification or perform identification themselves. Such agreements might be explicit (e.g. service agreement) or implicit (e.g. entering a facility indicating a clear intent to conduct a transaction). Systems used to monitor an indefinite number of people are excluded from the scope of this part of ISO 19092.

The techniques specified in this part of ISO 19092 are designed to maintain the integrity and confidentiality of biometric information and to provide authentication. However, ISO 19092 does not guarantee that a particular implementation is secure. It is the responsibility of the financial institution to put an overall process in place with the necessary controls to ensure that the process is securely implemented. Furthermore, the controls should include the application of appropriate audit tests in order to verify compliance with this part of ISO 19092.

Financial services — Biometrics —

Part 1: Security framework

1 Scope

This part of ISO 19092 describes the security framework for using biometrics for authentication of individuals in financial services. It introduces the types of biometric technologies and addresses issues concerning their application. This part of ISO 19092 also describes the architectures for implementation, specifies the minimum security requirements for effective management, and provides control objectives and recommendations suitable for use by a professional practitioner.

The following are within the scope of this part of ISO 19092:

- usage of biometrics for the authentication of employees and persons seeking financial services by:
 - verification of a claimed identity,
 - identification of an individual;
- validation of credentials presented at enrolment to support authentication as required by risk management;
- management of biometric information across its life cycle comprised of the enrolment, transmission and storage, verification, identification and termination processes;
- security of biometric information during its life cycle, encompassing data integrity, origin authentication and confidentiality;
- application of biometrics for logical and physical access control;
- surveillance to protect the financial institution and its customers;
- security of the physical hardware used throughout the biometric information life cycle.

The following are not within the scope of this part of ISO 19092:

- the individual's privacy rights and ownership of biometric information;
- specific techniques for data collection, signal processing and matching of biometric data, and the biometric matching decision-making process;
- usage of biometric technology for non-authentication convenience applications such as speech recognition, user interaction and anonymous access control.

This part of ISO 19092 provides the mandatory means whereby biometric information may be encrypted for data confidentiality or other reasons.

Although this part of ISO 19092 does not address specific requirements and limitations of business application employing biometric technology, subsequent parts of ISO 19092 may address these topics.

2 Conformance

A biometric authentication system may claim compliance to ISO 19092 if the implementation satisfies the management and security requirements identified in ISO 19092-1 and ISO 19092-2.

A biometric authentication system that utilizes the cryptographic message requirements recommended in ISO 19092-2 and which has implemented appropriate policies, practices and operational procedures shall comply with ISO 19092.

Compliance of many of the aspects of a biometric authentication system can be achieved by satisfying the management and security requirements specified in Clauses 9 and 10 and in ISO 19092-2, and verified if the implementation and its associated policies, practices and operational procedures meet the validation control objectives identified in Clause 11. An organization can document compliance to many operational aspects of ISO 19092 using the biometric event journal specified in Annex A.

3 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 10202-3, *Financial transaction cards — Security architecture of financial transaction systems using integrated circuit cards — Part 3: Cryptographic key relationships*

ISO 19092-2:—¹⁾, *Financial services — Biometrics — Part 2: Message syntax and cryptographic requirements*

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

4 Terms and definitions

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

4.1 adaptation

process of automatically updating or refreshing a reference template

4.2 attempt

submission of a biometric sample on the part of an individual for the purposes of enrolment, verification, or identification in a biometric system

NOTE An individual can be permitted several attempts to enrol, to verify, or to be identified.

4.3 binning

database partitioning based on information contained within (endogenous to) the biometric patterns

4.4 biometric

characterized as being biologically or behaviourally measurable, thus reliably distinguishing one person from another, so as to recognize the identity, or verify the claimed identity, of an enrollee

1) To be published.

4.5**biometric authentication**

process of confirming an individual's identity, either by verification or by identification

4.6**biometric data**

extracted information taken from the biometric sample and used to generate either a reference template or a match template

4.7**biometric identification**

one-to-many process of comparing a submitted biometric sample against some or all enrolled reference templates to determine an individual's identity

4.8**Biometric Policy****BP**

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

4.9**Biometric Practice Statement****BPS**

statement of the practices which an organization follows during the biometric template life cycle (e.g. creation, management, and destruction), including business, legal, regulatory and technical matters

4.10**biometric sample**

initial (raw) biometric data that is captured and processed

4.11**biometric system**

automated system capable of capturing, extracting, matching and returning a decision (match/non-match)

4.12**biometric verification**

process of comparing a match template against a specific reference template based on a claimed identity (e.g. user ID, account number)

4.13**capture**

acquisition of a biometric sample

4.14**claim of identity**

name or index of a claimed reference template or enrollee used by a biometric system for verification

4.15**claimant**

person submitting a biometric sample for verification

4.16**confidentiality**

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

[ISO/TR 13569:2005; ISO 15782-1:2003; ISO/IEC 13335-1:2004]

4.17

cryptographic exchange

secure transport or storage of data or cryptographic materials under the protection of a cryptographic key

4.18

decision policy

logic through which a biometric system provides match/non-match decisions, inclusive of the following elements:

- the biometric system's matching threshold;
- the number of match attempts permitted per transaction;
- the number of reference templates enrolled per claimant;
- the number of distinct biometric samples (e.g. different fingerprints) enrolled per claimant;
- the number of biometric technologies (e.g. fingerprint, voice) in which the claimant is enrolled;
- the use of internal controls in the matching process to detect like or non-like biometric samples.

NOTE Serial, parallel, weighted or fusion decision models in biometric systems can use more than one reference template in the match process for a given user (e.g. multiple-biometric systems as well as systems in which reference templates are created and stored from multiple fingerprints).

4.19

encryption

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

4.20

enrolment

process of collecting biometric samples from a person and the subsequent generation and storage of biometric reference templates associated with that person

NOTE See also **initial enrolment** (4.36) and **re-enrolment** (4.47).

4.21

Equal Error Rate

EER

probability or percentage of errors when the decision threshold of a system is set such that the false match rate is equal to the false non-match (historically crossover rate)

4.22

extraction

feature extraction

process of converting raw biometric data into processed biometric data for use in template comparison or reference template creation

4.23

face biometrics

biometric technology based on the distinctive characteristics of the face, inclusive of features in the visible spectrum, the infrared spectrum, or both

4.24

failure to acquire

failure of a biometric system to capture a biometric sample, or to extract biometric data from a biometric sample, sufficient to generate a reference template or match template

4.25**failure to enrol**

failure of a biometric system to capture one or more biometric samples, or to extract data from one or more biometric samples, sufficient to generate a reference template

4.26**False Acceptance Rate****FAR**

the probability, in a one-to-one system, that a biometric system will incorrectly identify an individual, or will fail to reject an impostor

NOTE For a positive (verification) system, it can be estimated by dividing the number of false acceptances by the number of impostor verification attempts.

4.27**False Match Rate****FMR**

rate for incorrect positive matches by the matching algorithm for single template comparison attempts

NOTE For a biometric system that uses just one attempt to decide acceptance, FMR is the same as FAR. When multiple attempts are combined in some manner to decide acceptance, FAR is more meaningful at the system level than FMR.

4.28**False Non-Match Rate****FNMR**

rate for incorrect negative matches by the matching algorithm for single template comparison attempts

NOTE For a biometric system that uses just one attempt to decide acceptance, FNMR is the same as FRR. When multiple attempts are combined in some manner to decide acceptance, FRR is more meaningful at the system level than FNMR.

4.29**False Rejection Rate****FRR**

probability that a biometric system will fail to identify a genuine enrollee

NOTE For a positive (verification) system, it can be estimated by dividing the number of false rejects by the number of enrollee verification attempts.

4.30**filtering**

partitioning a database through the use of exogenous information about the user not discernible from the biometric patterns, such as sex, age or race

4.31**finger geometry**

biometric technology based on the distinctive characteristics of the shape and dimensions of one or more fingers

4.32**fingerprint biometrics**

biometric technology (e.g. finger minutia or finger pattern matching) based on the distinctive characteristics of the friction ridges and valleys present on an individual's fingertips

4.33**hand geometry****hand identification**

biometric technology based on the distinctive characteristics of the shape and dimensions of the hand

4.34

impostor

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

4.35

information security

preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved

[ISO/IEC 17799:2005]

4.36

initial enrolment

process of enrolling an individual's biometric data for the first time, such that the individual shall provide a means of authentication, such as a password or ID in order to establish or confirm an identity

NOTE See also **enrolment** (4.20) and **re-enrolment** (4.47).

4.37

integrity

property of safeguarding the accuracy and completeness of assets

[ISO/IEC 13335-1:2004]

4.38

iris biometrics

biometric technology based on the distinctive characteristics of features found in the iris

4.39

match

process of comparing a match template against a previously stored reference template and scoring the degree of similarity or correlation between the two

4.40

match template

data, which represents the biometric measurement of a claimant, extracted from a claimant's biometric sample and used by a biometric system for comparison against one or more stored reference templates

4.41

multi-biometric authentication

biometric authentication using two or more different biometric types

NOTE For example, finger biometrics with iris biometrics or voice biometrics with face biometrics.

4.42

multi-factor authentication

authentication using two or more factors:

- knowledge factor, "something an individual knows";
- possession factor, "something an individual has";
- biometric factor, "something an individual is or is able to do".

4.43

one-to-many

biometric identification

4.44**one-to-one**

biometric verification

4.45**palm biometrics**

biometric technology based on the distinctive characteristics of features found in the palm of the hand, inclusive of ridge/minutiae information and/or palm lines

4.46**raw biometric data**

captured, unprocessed biometric data (e.g. fingerprint image or audio stream) from a sensor device, in digital form, suitable for subsequent processing to create a biometric sample or template

4.47**re-enrolment**

process of enrolling an individual's biometric data where the same or other biometric data has been enrolled at least once

NOTE See also **enrolment** (4.20) and **initial enrolment** (4.36).

4.48**reference template**

data which represents the biometric measurement of an enrolee, extracted from an enrolee's biometric sample and typically stored and used by a biometric system for comparison against subsequently submitted match templates

4.49**registration**

process in which a person proves his/her identity by presenting credentials to the biometric service provider before being allowed to enrol, and assigns an electronic identifier

4.50**retinal biometrics**

biometric technology based on the distinctive characteristics of features found in the retina

4.51**risk management**

coordinated activities to direct and control an organization with regard to risk

[ISO/IEC Guide 73:2002]

4.52**score**

numerical representation of the degree of similarity between two matched templates

NOTE The specific method by which a biometric score is generated, as well as the probability of its correctly indicating a true or false match, is generally propriety to each biometric vendor

4.53**signature verification biometrics**

biometric technology based on the distinctive characteristics of features found in the dynamics of a hand-written signature or other signed symbols

4.54

single-factor authentication

authentication using only one factor:

- knowledge factor, “something an individual knows”;
- possession factor, “something an individual has”;
- biometric factor, “something an individual is”.

4.55

template

data which represents the biometric measurement of an individual, used by a biometric system to execute biometric matches

NOTE See **match template** (4.40) and **reference template** (4.48).

4.56

threshold

point above which the degree of similarity between two compared templates is sufficiently high to constitute a “match”, and below which the degree of similarity between two compared templates is sufficiently low to constitute a “non-match”

NOTE Thresholds can often be adjusted at an administrative level to decrease the **False Match Rate** (4.27) or to decrease the **False Non-Match Rate** (4.28).

4.57

voice biometrics

biometric technology based on the distinctive characteristics of acoustic information found in the voice of a speaker

5 Symbols and abbreviated terms

AES	Advanced Encryption Standard
ATM	Automated Teller Machine
BISMS	Biometrics Information Security Management System
CA	Certification Authority
DEA	Data Encryption Algorithm
DES	Data Encryption Standard
DSV	Dynamic Signature Verification
IC	Integrated Circuit
ICC	Integrated Circuit Card
ID	Identification
KEK	Key Encryption Key
PKI	Public Key Infrastructure

6 Biometric technology overview

6.1 Introduction

Biometric technology addresses the problems associated with confirming the identity of an individual for the purposes of financial transactions. The registration processes are a prerequisite for any formal biometric enrolment. Each person shall prove his/her identity by means of credentials to the biometric service provider before being allowed to enrol. This provides assurance that the biometric reference template is actually bound to the identity of the individual who has enrolled.

Biometric identification leverages the universally recognized fact that certain physiological or behavioural characteristics can reliably distinguish one person from another. Biometric technology includes both the automatic collection and the comparison of these characteristics. The digital representations of these characteristics are stored in an electronic medium, and are later used to confirm the identity of an individual. A typical authentication process using biometric technology consists of the following basic steps:

- a) capture the biometric data,
- b) evaluate the quality of the captured biometric data and recapture if necessary,
- c) process the captured biometric data, and
- d) match the processed biometric data with a previously enrolled template(s) to determine if a match exists; this matching can be done for biometric verification or biometric identification.

There are three basic biometric processes: enrolment, verification and identification.

- Enrolment is the process of collecting biometric samples from a person and the subsequent generation and storage of biometric reference templates associated with that person. Enrolment may entail the collection of other information about the individual, which links them to an organization, an account, or a set of privileges. In cases where duplicate enrolment is not allowed, enrolment may be preceded by a one-to-many comparison to make sure that the individual is not already in the database, perhaps under another name. If no match is found, the template and its associated information may be added to the individual's respective database entries. (See also 9.3.)
- Verification is a "one-to-one" comparison. This process entails the comparison of a match template generated from a newly captured sample with a previously generated reference template stored in a database or on an ID card. If the newly captured sample matches the previously generated template, the claim of identity is confirmed or verified.
- Identification is a "one-to-many" comparison. This process entails the comparison of a match template generated from a newly captured sample with all of the templates in the database. It is most often used to determine whether a person has previously enrolled in the system. Some systems use an external qualifier (e.g. telephone number) to narrow the search and subsequent identification to "one-to-few".

The advent of modern computing techniques is making the use of biometric technology for the purposes of identification a viable option in many areas. The characteristics which can be used to represent an individual include fingerprints, voiceprints, iris patterns, hand geometry, facial image, retinal patterns and signature verification. These seem to be the current mainstream biometric technologies, and a brief description of these techniques is given in the following paragraphs. However, these are not the only biometric characteristics available today. Others include palm identification, head acoustics, wrist vein geometry, body odour, ear shape and keystroke dynamics. As technology advances, the list of viable characteristics may well expand.

6.2 Fingerprint biometrics

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 Henry types and sub-types (i.e. fingerprint patterns such as loops, whorls, and arches) as well as determining

identity by matching 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 key points (such as the core and the deltas). Fingerprint biometrics is capable of both verification and identification.

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. 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. Many fingerprint systems are being marketed by many companies, and the cost, size and speed of this technology have made significant advances in this competitive environment

6.3 Voice biometrics

Voice biometrics (also called “speaker recognition”) dates back five decades. Early systems, pre-dating digital computing, used the output of several analogue filters, which were averaged over time for matching. Current digital speaker recognition systems model 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 any of three styles of spoken input: text-dependent, text-prompted, and text-independent speech. Most speaker verification applications use text-dependent input, which involves selection and enrolment of one or more voice passwords. Text-prompted systems ask users to repeat specific words, phrases, or numbers. Text-prompted input is used where there is concern about tape-recorded impostors. Text-independent input is free-flowing speech.

Voice biometrics can be used for challenge-response type speaker verification, categorized in ISO/IEC 7816-11 as “dynamic biometric verification”. 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.

Ambient noise levels can be an impediment to the collection of initial and subsequent voice samples. Voice changes due to ageing also need to be addressed by voice biometrics systems; adaptation can be employed to evolve the voice template along with changes in the verified speaker's voice. Many companies market speaker recognition engines, often as part of large voice processing, control and switching systems. Capture of the biometrics is seen as non-invasive. The technology needs little additional hardware and can leverage existing microphones and voice-transmission technology. This provides functionality over long distances via ordinary telephones (wire line or wireless). However, performance is negatively affected by changes between enrolment and sampling in the microphone type or the transmission path.

6.4 Iris biometrics

The iris of the eye is the coloured portion of the eye surrounding the pupil. Iris imaging uses distinctive anatomical features such as corona, crypts, filaments, freckles, pits, radial furrows, and striations that make up the complex iris patterns. Iris biometrics entails illumination of the eye, capture of the resulting image, and location of distinctive features through specialized video cameras. Iris biometrics is capable of both verification and identification.

Iris images can be acquired automatically and with reasonably little effort from a distance of more than 0,33 m from the camera. Iris biometrics systems utilize automatic eye detection and advanced camera technology. Iris biometrics systems are much easier for the public to use than retinal systems.

The iris, being naturally well protected behind the cornea, appears to be stable over long periods (decades) according to medical literature. Iris imaging is not perceived as highly invasive, since the minimum distance, even for less-sophisticated iris identification systems, is between 75 mm and 100 mm from the sensor. Iris images are unaffected by common contact lenses, but can be affected by “designer” contacts. Reflections caused by eyeglasses and sunglasses can also be a problem.

6.5 Retina biometrics

The retina is a structure in the interior of the eye. Retinal biometrics leverages the pattern of blood vessels on the retina. Retinal biometrics entails illumination of the eye, capture of the resulting image, and location of distinctive features through specialized video cameras.

Accurate retinal imaging requires almost perfect alignment of the eye with the scanning device, which requires the eye to be in close proximity to the scanner. This requires a great deal of effort and training, and can lead to high levels of enrolment and non-matching errors. At the same time, this contributes to the technology's historically low false match rate. Retina biometrics is capable of both verification and identification.

Retinal patterns are highly distinctive, but the retinal structure may change during the lifetime of the person. The requirement for close proximity to the retinal imager, as well as the beam of light shone into the eye, is perceived as unpleasant by many.

6.6 Face biometrics

Biometric technology often involves the identification or verification of a person by their facial image. Most face biometrics solutions utilize images captured in the visible spectrum using standard camera technology. An alternative approach, known as facial thermography, uses an infrared camera to capture the unique heat emission patterns made by people's faces.

The visible light systems extract features from captured facial image(s). Approaches to modelling facial images in the visible spectrum include Principal Component Analysis, Local Feature Analysis, neural networks, elastic graph theory, and multi-resolution 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. Local Feature Analysis locates and maps key feature points of the face, similar to fingerprint minutiae extraction. Face biometrics is capable of both verification and identification.

Challenges for facial identification in the visual spectrum include reducing the impact of changes in pose, expression, hairstyle, facial hair, makeup and lighting. 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 and accepted by most users. In the visible spectrum, an untrained operator can also assist the system when identification is uncertain.

6.7 Hand geometry biometrics

Hand geometry has been used for physical access control and time and attendance systems for over two decades. Hand geometry systems use a camera array to scan the shape of the hand from different directions. Sensors determine when the hand is in correct alignment.

Hand geometry uses the dimensions and shape of the hand, fingers and knuckles to form an identifying series of numbers. This template is one of the smallest, requiring only 9 bytes for storage. Operation requires use of a token or a PIN, as the technology operates only in verification mode.

Users with arthritis and rheumatism, as well as those with missing fingers or excessively large hands, could have difficulties. Hand geometry is convenient to use and requires little training. The process of using a hand scanner is perceived as non-invasive and acceptable to the public. A related biometric technology is finger geometry, scanning and extracting features only from a few fingers, as opposed to the entire hand.

6.8 Signature biometrics

Hand-written signatures can be identified by the way the signature looks or 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 Dynamic Signature Verification (DSV). These systems capture the way we sign our names, using features such as the angle of the pen, the time to complete the signature, the acceleration and velocity of the pen, the pressure while signing, and how often the pen is lifted from the page. 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.

The sensing equipment can be highly sensitive and prone to wear and tear over time, and therefore may prove to be maintenance intensive. Since DSV is not based on a static image, forgery is very difficult. Several companies market DSV systems and public acceptance of signature verification is high, since hand-written signatures are currently one of the most accepted means of asserting identity.

6.9 Vein biometrics

Vein authentication uses the blood vessel pattern of the veins in the subcutaneous tissue of the human body to discriminate between individuals. A vein pattern is read using near-infrared light. When a hypodermic vein is irradiated with near-infrared light, the reduced haemoglobin contained in the vein absorbs near-infrared light and the hypodermic vein creates a shadow on an 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.

In practical terms, 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 help guide the 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 very difficult.

Many products for vein authentication of a palm, a finger or the back of a hand, are already employed by ATMs of multiple financial service companies ²⁾ and as access control systems.

7 Technological considerations

7.1 Biometric system properties

For applications in the financial services, the following biometric system properties should be considered:

- public acceptance and policy considerations,
- resistance to fraud (see Annex C),
- universality of the chosen biometric characteristic,
- uniqueness of the chosen biometric characteristic,
- accuracy of the biometric system,
- stability of the biometric characteristic,
- template storage requirements (i.e. template size),

2) In Japan, since December 2005, the vein authentication technology of a palm or a finger is employed on ATMs of financial institutions, including some major banks and several regional banks.

- system validation ability,
- speed of comparison between the claimant sample and the enrolled template, and
- environmental and interface factors.

7.2 Universality

In order for a biometric system to be of value, nearly all people in the target population should be able to successfully use that system. A small number of exceptions may be possible, providing that an alternative method is available to authenticate or recognize those people who are unable to use the biometric system. Care shall be taken in the design and administration of that alternative method, so that it does not become a point of weakness or vulnerability in the system.

While vendor claims may be misleading, measurable error rates are associated with all biometric technologies. Most of these errors come from two classes of users:

- a) individuals who cannot provide the biometric feature required by the sensor;
- b) individuals who are unable to give consistent or high-quality samples, resulting in false non-matches.

Such individuals are referred to as “outliers” in the biometric industry. Experience suggests that they either do not have a repeatable biometric measurement, or experience chronically a “failure to acquire” system error.

The percentage of outliers differs by technology and vendor. The use of multiple biometrics is a potential solution to the outlier problem, since the overall probability of an individual being an outlier across two or more biometrics is smaller than the probability for a single biometrics. Alternatively, other identification factors can be used as a fallback, such as the PIN, for users not possessing the biometric feature of interest.

While alternative methods are often necessary to provide for universal authentication, these alternatives might undermine overall system security. The use of passwords as a fallback, for example, may provide the incentive for an attacker to fail his/her biometric match on purpose, in order to access a less robust authentication mechanism.

7.3 Distinctiveness

Distinctiveness describes how reliably the biometric characteristic is measurably different for each individual in the population. In an ideal system, there would be no ambiguity: the measured biometric feature from each individual in the population would be different from that of every other individual. This can only occur if the feature itself is unique to each individual, who at least requires that the number of permutations be large enough to accommodate the population³⁾, and if the biometric system can measure the feature with enough detail and repeatability to produce a unique electronic analogue of that feature.

Experience and studies provide some idea of the distinctiveness of most of the popular biometric characteristics. For example, fingerprints have been studied for many years, and there is a consensus that fingerprint patterns are unique among individuals. More recent studies suggest that iris and retinal patterns are also unique. On the other hand, the facial features of identical twins, for example, may not be unique. The properties of each biometric technology are therefore different, and should be evaluated to determine which of them provide the level of distinctiveness required for a given application.

7.4 Accuracy

Biometric techniques are subject to statistical error, such that impostors may be granted access to protected resources that legitimate users are prevented from accessing. The probability that a biometric system will fail to reject an impostor in a 1:1 verification attempt, or will incorrectly identify an individual in a 1:N identification

3) A template size of at least $2^{32} \approx 4$ billion permutations would theoretically accommodate the earth's population.

attempt, is the system's False Match Rate (FMR). The probability that a biometric system will fail to verify an enrolled individual in a legitimate 1:1 verification attempt, or will fail to identify an enrolled individual in a 1:N identification attempt, is the system's False Non-Match Rate (FNMR). The techniques discussed in this part of ISO 19092 are all prone to some level of false matching and false non-matching.

A system's FMR and FNMR are inversely related, such that adjusting biometric system security settings to reduce the FMR results in an increased FNMR, and vice versa. Two biometric templates are determined to "match" or "non-match" based on a comparison between

- a) the score that results from the match attempt, and
- b) the system's match threshold.

Strictly speaking, a system's FMR and FNMR are not "adjusted" by an administrator. Instead, the administrator adjusts a single threshold above which two templates are declared a match and below which two templates are declared a non-match. It is therefore impossible to adjust one error rate without impacting the other: both error rates are a function of a single threshold.

A deployer's operating environment will generally dictate which of the error types should be limited, at the expense of potentially increasing the other error type. For example, a high-security facility will usually minimize the system FMR at the expense of increasing the system FNMR, whereas a customer service facility will usually minimize the FNMR at the risk of increasing the FMR.

Because of the relationship between FMR and FNMR, a system's FMR is only meaningful when provided in conjunction with its FNMR, and vice versa. Any system can claim a FMR of 0 % by simply rejecting every attempt, or a FNMR of 0 % by accepting every attempt. An ideal biometric system will offer simultaneously low FMR and FNMR.

The point at which a biometric system's FMR equals its FNMR is the Equal Error Rate (EER) or Crossover Error Rate.

NOTE 1 Some biometric systems do not allow threshold adjustments and do not use EER [17].

This rate provides a useful snapshot of overall matching accuracy, as a system with a low EER is more likely to operate accurately than one with a high EER. However, few deployers will actually implement a system in which false match and false non-match rates are identical. Most will choose to emphasize either convenience or security, depending on their operating environment. When comparing the accuracy of different biometric technologies, deployers should evaluate what constitutes acceptable levels of both false matching and false non-matching, and then determine what technology or technologies are capable of providing the required level of performance for both metrics.

NOTE 2 FMR and FNMR cannot be used alone to determine overall system accuracy: a system's failure-to-enrol rate, or the percentage of users unable to provide sufficiently distinctive or replicable biometric data for enrolment, is a critical element not captured by matching error rates.

Capabilities of certain biometrics allow them to be deployed for the purposes of identification, or "single-factor authentication." Single-factor authentication does not require that the individual provide a unique identifier in the form of a card, token or username, with major implications for system security and convenience. These issues are discussed further in C.8.

Error rates can be generated through independent testing or through vendor-provided testing. In either case, published error rates may only be reflective of operation in a strictly controlled test environment, and may not be indicative of performance in a deployment environment, subject to decision policy. Decision policy is the logic through which a biometric system provides match/no match decisions, inclusive of implementation-specific factors. In order to gauge a biometric system's real-world performance, the system's error rates should be evaluated in conjunction with its decision policy.

One of the major factors in a biometric system's decision policy is the number of attempts permitted for verification or identification. In biometric systems, an "attempt" is the act of an individual providing a usable biometric sample — i.e. a single fingerprint, voice pattern, or iris image — to a biometric system.

NOTE 3 In certain biometric systems, an attempt consists of comparison of multiple biometric samples acquired over a brief period. Facial-scan systems can acquire multiple facial images over the period of several seconds, generate match templates with each image, and declare a match if any of the acquired images exceed the required threshold. In this case, the “attempt” can continue until the system times out after a certain duration.

Most biometric systems allow an individual multiple attempts to be verified or identified before timing out or preventing further attempts, e.g. an individual may be allowed to place a fingerprint on a scanner up to three times in order to verify against his or her enrolment. A common decision policy is to grant access if any of the three attempts is successful. Under this decision policy, the system’s effective FNMR may be lower than its single-attempt FNMR, i.e. the user is more likely to be verified at some point in the verification sequence given the additional attempts. However, this decision policy increases a system’s effective FMR, because an impostor may have multiple chances to provide biometric data in an effort to defeat the system.

Another factor in a biometric system’s decision policy is the number of enrolment templates associated with a given user. Many biometric systems acquire two enrolment templates from a user, such as from the right and left fingerprints, in order to mitigate the impact of injuries and to reduce incidents of false non-matching of authorized users. If a system allows a user to verify against either of his or her enrolled templates, the system’s effective FNMR may be lower than its single-attempt FNMR, i.e. the user is more likely to be verified against one of his or her enrolled templates. However, this decision policy increases a system’s effective FMR, because an impostor may have multiple chances to match against enrolled biometric data.

Other decision policy elements that can impact a system’s accuracy include the following:

- the number of distinct biometric samples (e.g. different fingerprints) enrolled per claimant;
- the number of biometric technologies (e.g. fingerprint, voice) in which the claimant is enrolled;
- the use of internal controls in the matching process to detect like or non-like biometric samples, e.g. comparing templates derived from two subsequent match attempts to determine if the individual is placing different fingers in an attempt to falsely match;
- the use of serial, parallel, weighted or fusion decision models in biometric systems that utilize more than one reference template in the match process for a given user (e.g. multiple-biometric systems, as well as systems in which reference templates are created and stored from multiple fingerprints).

Secure biometric system implementation requires that deployers evaluate the impact of decision policy on the FMR and FNMR in order to determine how well their system will perform when deployed. A biometric system’s effective False Match Rate and its effective FNMR represent its error rates with all elements of a deployer’s decision policy taken into consideration. The overall decision policy (including thresholds) is set according to the needs of the organization, based upon a risk assessment.

7.5 Performance evaluation

When evaluating the performance of biometric products, it is important to understand the different factors that can influence the measured FMR and FNMR (see also C.5). Reported performance numbers for different products may have been measured under different circumstances, and thus they cannot be directly compared. The factors below should be taken into consideration.

- **Who were the users in the test, and how were they selected?** Ideally, the users should be chosen at random from a population that is representative of the people who will use the system in the real application environment. In some cases, however, the test users do not accurately represent the real-world users. 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 can influence the performance with the chosen biometric system.
- **How were the test users trained?** The training for the testers should be as close as possible to that anticipated for users of the real system. The testers are often more carefully coached than the real users will be, either intentionally (to improve measured performance) or unintentionally (due to the enthusiasm of the vendor for his/her own product). A related issue is how long the test group used the system before the formal measurement period began. Typically, performance will be lower when the users begin using the system, and will rise and stabilize as they get accustomed to it.

- **What thresholds were used during the test?** Because false match and false non-match rates between samples and stored templates are dependent upon threshold settings, system FMR and FNMR encountered during testing will similarly be affected by the chosen thresholds. FMR and FNMR should be reported together at a common threshold.
- **How many attempts are allowed per verification session?** Most measurements are based on single attempts to verify identity with the biometric system. However, some are based on the overall results of a “session” in which the user is permitted several tries. The system decision policy, including the number of allowed attempts per verification session, will allow for various system FNMR and FMR to result from the same single-comparison false match and false non-match rates. Clearly, the FNMR will be lower and the FMR will be higher if the user is given more than one try at verification.
- **Were problem users systematically eliminated from the test?** It is common for some users to experience a “failure to acquire” during enrolment. This is often called a “failure to enrol.” If enrolment requirements are placed high, problem users can be systematically eliminated from the test at enrolment. Of course, eliminating problem users will lower measured false non-match rates later in the test and result in better system performance.
- **What is the motivation to succeed at impersonating another user?** In some biometric systems, a user has a better chance of achieving a false match if motivated to do so, e.g. the user may have a better chance of impersonating another user’s signature, voice or keyboard dynamics if he/she is trying very hard to do so. Measurements of FMR can therefore be influenced by the testing method. In some tests, users are directly rewarded if they can successfully forge another user’s identity. In other tests, there is no reward. Finally, some false match tests are carried out simply by cross-testing a database of collected biometric data, in order to see if any of the samples can be verified as a match to any other sample which came from a different person.
- **How did the test conditions compare with those for the real application?** Did the test subjects use the system while seated in a comfortable room? If so, will the real application involve verification outdoors in potentially bad weather or in the dark? Will users have to verify while standing? Will they be clothed differently in some way, such as in heavy winter coats, that might in some way affect verification performance? These are important factors in determining whether the test results will accurately match those obtained in the real world.
- **Was the test organization impartial?** Some tests are run by independent organizations. Others are run by the vendor who sells the biometric product or by some other organization with a stake in making the product look good, or perhaps bad. An independent test organization is more likely to test products in a way that is unbiased, rather than performing the test under the best-case circumstances for that particular product or technology.
- **Has there been a change in the product since the test was performed?** Products constantly change. The test results you see may have been measured with a version of the product that differs from what is available today. Frequently this means that performance will improve, or that performance will be the same, but with a reduction in cost. Although less likely, it is also possible, however, that changes in hardware or software can reduce performance.

It is important to understand these issues before choosing a biometric product for your application. Biometric performance depends upon the precise conditions of the installation and the users, can be difficult to measure, and may be subject to much more variation than performance measurements of other products, e.g. it is much easier to measure the number of transactions per hour that a computer system can support, or the access time for a disk drive. When selecting a biometric system, be sure you understand how performance was measured, and how that method relates to the way the system will be used in your application.

There is no substitute for testing in an environment that replicates the actual application environment. Biometrics vendors cannot replicate the conditions of all potential customers, and it should be expected that the vendors have a natural bias to portray their products favourably. Thus, the customer should ultimately test to understand how a system would perform under their specific conditions.

7.6 Interoperability

Biometric templates issued by financial institutions should be used in a manner that is consistent with the biometric information management policy and practices of the institution. The common event journal syntax specified in ISO 19092-2 helps to simplify the auditing of biometric events and facilitates the effective management of biometric information systems.

8 Basic principles of biometric architectures

8.1 Biometric system model

All biometric systems have the common function of recognizing individuals by matching some personal physical characteristic with the stored information about that same characteristic. The methods, applications, and implementations of biometric systems vary widely, and in the context of biometric standards it is important to understand the biometric system model and basic approaches that are common to most applications.

All biometric systems are composed of the following subsystems:

- data collection;
- signal processing (feature extraction);
- matching;
- storage;
- decision;
- transmission.

NOTE For dynamic biometric verification, a “challenge presentation” subsystem is used.

Transmission is the movement of biometric data between two components that are not physically collocated within the same tamper-resistant security module. Transmission can occur between any two components, depending on the specific vendor implementation, and may not exist in some systems.

Any biometric system operates in an environmental context, which shall be taken into consideration when evaluating security aspects of the system. 11.2 illustrates the two major domains of any biometric system, i.e.

- a) the physical domain, in which resides the subject to be verified or identified, and
- b) the logical domain, in which the computational processing of the biometric data takes place.

The data collection device provides the bridge from the physical domain to the electronic processing domain.

Furthermore, some biometric technologies may have low enough crossover error rates to be suitable for large-scale single-factor authentication. Single-factor authentication has major implications from the points of view of security and convenience (see C.4.3).

Each of the major components is described in more detail in 8.2 to 8.8.

8.2 Data collection subsystem

The data collection subsystem contains the input device or sensor that reads the biometric information from the user and converts it to a form suitable for processing by the remainder of the biometric system.

It is the link from the physical domain to the logical domain. Examples include a variety of transducers, such as a video camera, a fingerprint scanner, a special signature pen or tablet, a microphone and other input devices specific to the chosen biometric characteristic to be measured. The output of this subsystem is raw biometric data, which may be processed locally or may be transmitted to another location.

To successfully recognize a user, the sampled biometric characteristic shall always be similar to the user's enrolled template to which it is compared. This imposes requirements on the design of the data collection sensor, and may impose training requirements for the users. Some characteristics change slowly over time, and biometric systems may employ adaptation in order to keep the stored reference template in step with those changes (see also C.7.3 and C.7). Re-enrolment of a user's record by provision of a new enrolment template for that individual on an overt basis (usually initiated by the application) may also be performed.

In use, the biometric feature is presented to a sensor, which converts the feature into an electronic signal suitable for further processing. All sensors in a given system shall be similar enough that a feature measured by one sensor will closely match the same feature measured at other sensors, so that the user can be recognized equally well at any location. This includes the requirement that the sensors shall be consistent over time, either by virtue of inherent stability, or through use of automatic calibration. Some systems include automatic quality control features in the sensors or signal processing paths, and these systems can detect poor-quality signals that might otherwise increase the false non-match rate.

The performance and output of the data collection subsystem is impacted by changes in any of the following:

- the underlying biometric pattern,
- the presentation of the pattern to the sensor,
- the performance of the sensor itself, and
- the surrounding environmental conditions (e.g. lighting, background noise).

8.3 Transmission subsystem

The transmission subsystem provides the ability to send information between the data collection, signal processing, decision, storage and matching components. The connectivity provided may be point-to-point or networked, allowing one system to connect to multiple subsystems.

The system components that communicate may be local or remote to each other, within the same secure envelope, e.g. tamper-resistant security module (see Annex D), or in separate secure envelopes. The transmission subsystem may not necessarily be monolithic, but may actually be composed of a number of different transmission media, such as Ethernet, leased line, wireless, etc. These media may or may not provide security services, such as data confidentiality, data integrity and authentication of origin between the connected subsystems.

8.4 Signal processing subsystem

The signal processing subsystem receives the raw biometric data from the data collection subsystem, and transforms that data into the form required by the matching subsystem. The exact processing that takes place varies for different biometric characteristics that are measured, and for the biometric systems of different vendors.

The system may perform a quality analysis on the input signal to determine if it is satisfactory for use. If the signal fails the quality tests, it is rejected, and depending upon the enrolment policy, the user may need to supply another presentation of the biometrics.

Filtering may be applied to the signal in order to remove noise or other information that is extraneous to the matching process. This may include, for example, removing high- or low-frequency data from the signal.

The signal may be normalized in some way, e.g. the voltage level of an analogue signal may be adjusted to be within accepted limits, and a video image may be adjusted to standard levels of brightness and contrast.

Once the input signal has been satisfactorily adjusted, it will be analysed to extract features that are used by the matching subsystem. Some biometric systems compare raw data, and this step is not required. Feature extraction is performed to transform the raw data into a set of characteristics that will represent it to the matching process. The types of features vary with different biometric techniques. A fingerprint system typically looks for physical characteristics, such as branch and end points of the ridges; the system would extract a set of values where each one contained an indication of the type of feature found, the coordinates where it was found on the finger, and the angle of the ridge at that point. A voice biometrics system, on the other hand, might record such things as the energy in the different frequency components of the signal. The result of feature extraction is data that is much smaller and simpler to use than the original raw data signal.

Typically, once raw biometric data has been processed, it is not feasible to reconstruct the raw data from the processed sample or template.

8.5 Matching subsystem

The matching subsystem receives the processed biometric data from the signal processing subsystem and compares it with the biometric template from the storage subsystem. The matching subsystem has a key role in the biometric architecture.

The matcher is composed of the following sub-components:

- sequencer,
- match-scoring module, and
- adaptation module (optional).

The sequencer handles the sequencing of the activation of the match and adaptation modules and the transfer of matching scores to the decision subsystem to perform different functions.

The match-scoring module measures the similarity of a claimant sample with a template. Each comparison of a sample with a particular template results yield a score, which is a numeric value indicating how closely the sample and template match. The method of computing the score differs among biometric technologies, but typical methods include distance metrics (see [15]), probabilistic measures and normalized correlation. Ultimately, the score should be related to a given confidence of positive identification for the biometric subject, which can be factored into the overall business rules and risk policy for the financial institution authorization policy. This confidence value will be considered by the decision subsystem in implementing the administrator's authorization policy for the transaction, employing the biometrics as an authentication factor.

In the simplest form of verification, the sequencer provides the claimant sample and enrolment templates to the matcher, and passes this result to a decision subsystem, which returns a binary decision regarding whether the claimant is who he/she claims to be.

However, the interplay between the match-scoring module and the sequencer may be quite involved in systems that carry out identification, e.g. in an identification mode, the sequencer may take into account additional indexing or binning information about the claimant sample, in order to focus the computations of the matcher onto templates that are most likely to match the claimant sample. Feedback from the decision subsystem might also be invoked during the identification process to guide the search towards the likeliest match enrolment templates.

Some systems use the sequencer and matcher, with feedback from the decision subsystem to perform adaptation, to keep the enrolment templates up to date with gradually changing biometric characteristics for the user (see also C.7).

An application program (e.g. a transaction authorization system) uses the decision process result in various ways, depending on the purpose of that application program. The actions at this level are not a part of the decision subsystem itself, but are a part of that application program. Most often, the application program will grant the user some level of privilege if the decision indicates a match with the template belonging to the claimed identity. In other systems, however, the goal is to verify that the user is not in the template database, e.g. when a financial services employee attempts to enrol in a benefits program in which he/she is already a member, thus avoiding duplicate records. In this case, the application program will “accept” the user only if the decision subsystem indicates that there are no matches between the user’s sample and any template in the current database.

8.6 Decision subsystem

The decision subsystem receives a score from the matching subsystem and, by means of a confidence value based on business risks and risk policy, interprets the results of the score.

The decision subsystem returns a binary yes or no regarding the positive identification of the claimant, based on the score computed by the pattern matching subsystem. In the most common case, the decision is based on a single threshold. If the score is above the threshold, the system concludes that the user is indeed the individual owning the template. If not, the system indicates that the user is not that individual. In more complicated cases, the decision subsystem may require matches in one out of three submitted samples, or in higher security scenarios, for two out of three multi-biometric characteristics.

An application program (e.g. a transaction authorization system) uses this decision process result in various ways, depending on the purpose of that application program. The actions at this level are not a part of the decision subsystem itself, but are a part of that application program. Most often, the application program will grant the user some level of privilege if the decision indicates a match with the template belonging to the claimed identity. In other systems, however, the goal is to verify that the user is not in the template database, e.g. when an individual attempts to enrol in a benefits program. In this case, the application program will “accept” the user only if the decision subsystem indicates that there are no matches between the user’s sample and any template in the current database.

8.7 Storage subsystem

The storage subsystem maintains the templates for the enrolled users. It provides for the addition, deletion and retrieval of an enrolled template (or templates), as needed by the matching subsystem. The storage subsystem may contain a single template for a single user, or thousands of templates, depending on the system architecture and intended function.

For example, templates may be stored in:

- physically protected storage within the biometric device,
- a conventional database on a computer system, or
- portable tokens, such as smart cards.

The data stored for each user always includes that user’s template, but it may also include other information. It may also contain data that is completely unrelated to the biometric system, if the same database is used for purposes other than user authentication.

8.8 Portable tokens

When portable tokens, such as smart cards, are used in conjunction with biometrics, then any (or none) of the biometric subsystems described in Clause 8 may reside within the token. The most common card deployment models are (from lowest to highest token cost):

- “identity on card”, in which the token contains no biometric template or subsystem, and is used with an external biometric verification system to provide 2-factor authentication;

- “off-card matching”, in which the biometric storage subsystem contains one or more reference templates stored in the token, and where all other biometric subsystems are external to the token;
- “on-card matching”, in which the matching and storage subsystems are in the token and data collection is external to the token; the signal processing or decision subsystems may be in or external to the token;
- “self-contained card”, in which all the biometric subsystems (including the sensor) are in the token, and verification can be performed without any external system interaction.

The “identity on card” model does not differ significantly from a cardless biometric implementation with a central database. The token contains a unique value that has been associated with the reference template of the individual. The individual possessing the token provides this value to claim an identity. This value is used to simplify location of the individual's reference template in a template database, without the need to search by biometric matching. Together, the token and biometrics provide 2-factor authentication. This model minimizes the risk of a cardless implementation and token cost, but does not provide the benefits of decentralized template management.

The other three models remove the need for centralized template management and database support, by housing the reference template in the token. However, decentralized template storage increases the risk of alteration or substitution of the template by an attacker. This risk of tampering can be mitigated by the use of integrity objects defined in ISO 19092-2.

The additional risks and confidentiality concerns that come with publicly sharing reference templates apply to the “off-card matching” model. In this model, the token shall emit the individual's reference template to an external verification system. This exposure makes the template vulnerable to theft by “skimming” or other attacks.

The “on-card matching” model avoids the risks of template exposure associated with the “off-card matching” model. This model does not emit the reference template to external systems. Instead, the token receives biometric samples or matching templates, and emits only biometric match results and decision control information.

The “self-contained card” model largely avoids tampering and skimming risks, since the token does not transfer the reference template across an interface to external systems during verification. However, self-contained tokens are prone to frequent sensor failure due to rough handling and storage of tokens, poor quality sampling due to dirty or damaged sensors, and higher failure rates (both FMR and FNMR) due to poor sample quality and limited processing power.

9 Management and security requirements

9.1 Basic applications

There are three basic applications in a biometric system:

- a) enrolment (creating the biometric template used in later verification or identification functions);
- b) verification (the user claims an identity and offers a biometrics to prove that identity), and
- c) identification (the system searches a database looking for a match with the offered biometrics).

9.2 Core security requirements

This subclause defines the requirements for managing and securing biometric information for each application, for the transmission and storage of biometric information, and for maintaining the event journal for purposes of compliance and audit. The following core requirements apply to all applications and environments, wherever biometric information is used.