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

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.

---

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO 19092-1:2006
https://standards.iteh.ai/catalog/standards/sist/39f651e6-74e9-486c-949a-
31191a947eff/iso-19092-1-2006

Contents

Page

iTeh STANDARD PREVIEW

(standards.iteh.ai)

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*

v

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 enrolee

---

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 enrolee 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 enrolee

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

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO 19092-1:2006
https://standards.iteh.ai/catalog/standards/sist/39f651e6-74e9-486c-949a-
31191a947eff/iso-19092-1-2006

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