
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.

© 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.