INTERNATIONAL STANDARD

ISO 19092

First edition
2008-01-15

Financial services — Biometrics — Security framework

Services financiers — Biométrie — Cadre de sécurité

Reference number
ISO 19092:2008(E)

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 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

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

This first edition of ISO 19092 cancels and replaces ISO 19092-1:2006, of which it constitutes a minor revision, notably to remove references to the ISO 19092-2 project.

Introduction

This International Standard replaces ISO 19092-1:2006. When ISO 19092-1:2006 was published, it was expected that a second part of ISO 19092 (ISO 19092-2, *Financial services — Biometrics — Part 2: Message syntax and cryptographic requirements*) would subsequently be published. However, ISO 19092-2 was not completed due to a lack of consensus. As a result, ISO 19092-1:2006 has been updated into this International Standard, removing all references to ISO 19092-2 and incorporating some minor editorial corrections.

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 such technologies as finger image, voice identification, eye scan and 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 International Standard 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.

Biometrics can be used for human authentication for physical and logical access. Logical access can include access to applications, services, or entitlements. This International Standard 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 International Standard 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 this International Standard are those for a closed user group 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). Such systems that will be used to monitor an indefinite number of people are excluded from the scope of this International Standard.

The techniques specified in this International Standard are designed to maintain the integrity and confidentiality of biometric information and to provide authentication. However, this International Standard 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 International Standard.

Financial services — Biometrics — Security framework

1 Scope

This International Standard 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 International Standard 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 International Standard:

- 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 International Standard:

- 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 International Standard provides the mandatory means whereby biometric information may be encrypted for data confidentiality or other reasons.

Although this International Standard does not address specific requirements and limitations of business applications employing biometric technology, other standards may address these topics.

2 Conformance

A biometric authentication system may claim compliance to this International Standard if the implementation satisfies the management and security requirements identified in this International Standard.

A biometric authentication system that utilizes the cryptographic message requirements recommended in this International Standard and that has implemented appropriate policies, practices and operational procedures shall comply with this International Standard.

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 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 this International Standard 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/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
biometrics
measurable biological or behavioural characteristic, which reliably distinguishes one person from another, used to recognize the identity, or verify the claimed identity, of an enrolee

4.5
biometric authentication
process of confirming an individual’s identity, either by verification or by identification