INTERNATIONAL STANDARD

ISO/IEC 19792

First edition
2009-08-01

Information technology — Security techniques — Security evaluation of biometrics

Technologies de l'information — Techniques de sécurité — Cadre de la sécurité pour l'évaluation et le test de la technologie biometrique

Reference number
ISO/IEC 19792:2009(E)

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

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/IEC 19792 was prepared by Technical Committee ISO/TC JTC1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

Information technology — Security techniques — Security evaluation of biometrics

1 Scope

This International Standard specifies the subjects to be addressed during a security evaluation of a biometric system.

It covers the biometric-specific aspects and principles to be considered during the security evaluation of a biometric system. It does not address the non-biometric aspects which might form part of the overall security evaluation of a system using biometric technology (e.g. requirements on databases or communication channels).

This International Standard does not aim to define any concrete methodology for the security evaluation of biometric systems but instead focuses on the principal requirements. As such, the requirements in this International Standard are independent of any evaluation or certification scheme and will need to be incorporated into and adapted before being used in the context of a concrete scheme.

This International Standard defines various areas that are important to be considered during a security evaluation of a biometric system. These areas are represented by the following clauses of this International Standard:

— Clauses 4 and 5 of this International Standard give an overview of all terms, definitions and acronyms used,

— Clause 6 introduces the overall concept for a security evaluation of a biometric system,

— Clause 7 describes statistical aspects of security-relevant error rates,

— Clause 8 deals with the vulnerability assessment of biometric systems and

— Clause 9 describes the evaluation of privacy aspects.

This International Standard is relevant to both evaluator and developer communities.

— It specifies requirements for evaluators and provides guidance on performing a security evaluation of a biometric system.

— It serves to inform developers of the requirements for biometric security evaluations to help them prepare for security evaluations.

Although this International Standard is independent of any specific evaluation scheme it could serve as a framework for the development of concrete evaluation and testing methodologies to integrate the requirements for biometric evaluations into existing evaluation and certification schemes.

This International Standard refers to and utilizes other biometric standards, notably those for biometric performance testing and reporting from ISO/JTC1 SC 37. These standards have been adapted as necessary for the specific requirements of biometric security evaluation.

2 Conformance

To conform to this International Standard, a security evaluation of a biometric system shall be planned, executed and reported in accordance with the normative requirements contained herein.

This International Standard describes the specific aspects of a security evaluation of a biometric system in terms of

— statistical error rates (see Clause 7),

— biometric-specific vulnerabilities (see Clause 8), and

— privacy (see Clause 9)

As some evaluation schemes that adopt this International Standard may not address all of the aforementioned aspects it shall further be possible to claim conformance to parts of this International Standard. In this case a security evaluation of a biometric system shall be planned, executed and reported in accordance with a subset of the normative requirements of this International Standard. In this case the requirements that are addressed shall be clearly identified.

Note that conformance to this International Standard is limited to the adoption of the biometric evaluation methodology described and adherence to the specified normative requirements. Conformance does not include scheme related issues such as action to be taken in the event that a system under evaluation fails to meet security relevant evaluation criteria or targets. The overarching scheme is responsible for specifying this action, which could include, for example:

— outright evaluation failure,

— restatement of evaluation criteria or targets to match achieved results, or

— development of a system under evaluation to meet specified evaluation criteria or targets.

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/IEC 19795-1:2006, *Biometric performance testing and reporting — Part 1: Principles and framework*