International Standard

ISO/IEC 19792

# Information security, cybersecurity and privacy protection — General principles, requirements and guidance for security evaluation of biometric systems

Second edition
2025-06

Reference number
ISO/IEC 19792:2025(en)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

# Contents

Page

# Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

This second edition cancels and replaces the first edition (ISO/IEC 19792:2009), which has been technically revised.

The main changes are as follows:

- the structure has been harmonized with general security evaluation methodology;
- the title has been changed from “Security evaluation of biometrics” to “General principles, requirements and guidance for security evaluation of biometric systems”, to align with the ISO/IEC 19989 series, the ISO/IEC 15408 series and the ISO/IEC 18045.

Any feedback or questions on this document should be directed to the user’s national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

# Introduction

This document 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 document are independent of any evaluation or certification scheme. If the requirements of this document are intended to be used in such a scheme, it will be necessary to adapt and incorporate them into the scheme before use.

This document defines various areas that are important to consider during a security evaluation of a biometric system. These areas are represented by the following clauses:

- Clause 5 explains the outline of security evaluation of biometric systems;
- Clause 6 overviews the threats and vulnerabilities to biometric systems that should be considered for the evaluation;
- Clause 7 describes the evaluation of biometric specific vulnerabilities related to recognition performance;
- Clause 8 deals with the evaluation of biometric specific vulnerabilities related to presentation attack detection;
- Clause 9 overviews the evaluation of privacy.

This document is relevant to both evaluator and developer communities. It shows how a security evaluation of a biometric system is performed. It serves to inform developers of the requirements for biometric security evaluations to help them prepare for security evaluations.

Although this document is independent of any specific evaluation scheme, it serves as a framework for developing concrete evaluation and testing methodologies that integrate the requirements for biometric evaluations into existing evaluation and certification schemes.

This document refers to and utilizes other biometric standards, notably those for biometric performance testing and reporting from ISO/IEC 19795-1, and the evaluation of presentation attack detection from the ISO/IEC 30107 series. These standards have been applied as necessary for the specific requirements of biometric security evaluation.

This document can also be used by organizations such as developers and procurers of biometric systems or devices to set proper security requirements for biometric systems or devices.

This document focuses mostly on the cases of complete biometric systems for verification or identification scenarios. However, the evaluation principles can be used entirely or partly for other cases such as: subsystems (e.g. presentation attack detection component, comparison component), other biometric scenarios (e.g. enrolment, duplicate enrolment check, white listing, black listing, quality assessment) or other biometrics-related processing aspects (e.g. emotional estimation, age estimation).

This document can be seen as an introduction to the ISO/IEC 19989 series, which covers the security evaluation of biometric products based on the ISO/IEC 15048 series. In addition, this document provides general guidance to design and execute security evaluation methodologies of biometric systems that are not aimed for evaluation conformant to ISO/IEC 15408 series.

This document does not address the vulnerabilities that are common to IT systems in general. For example, unprotected biometric data, biometric references, or comparison decisions, with which an attacker can tamper in order to impersonate someone else, are such vulnerabilities and are subject to evaluation under a general methodology, not specific to biometrics, such as the one specified in ISO/IEC 15408-1. However, general vulnerabilities associated with the information handled by the biometric system can employ system specific countermeasures which are addressed in Clauses 6 and 8.

# Information security, cybersecurity and privacy protection — General principles, requirements and guidance for security evaluation of biometric systems

## 1 Scope

This document specifies general principles, requirements and guidance for a security evaluation of a biometric system.

This document provides an overview of the main biometric-specific aspects, i.e. recognition performance, presentation attack detection and privacy, and specifies principles to consider for the security evaluation of a biometric system.

This document does not address the non-biometric aspects which can form part of the overall security evaluation of a system using biometric technology (e.g. requirements on databases or communication channels).

## 2 Normative references

There are no normative references in this document.