INTERNATIONAL STANDARD

ISO/IEC 19989-2

First edition
2020-10

Information security — Criteria and methodology for security evaluation of biometric systems —

Part 2: Biometric recognition performance

Sécurité de l'information — Critères et méthodologie pour l'évaluation de la sécurité des systèmes biométriques — Partie 2: Efficacité de reconnaissance biométrique

Reference number
ISO/IEC 19989-2:2020(E)

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).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see http://patents.iec.ch).

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.

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

A list of all parts in the ISO/IEC 19989 series can be found on the ISO website.

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.

Introduction

Biometric systems can be subject to presentation attacks where attackers attempt to subvert the system security policy by presenting their natural biometric characteristics or artefacts holding copied or faked characteristics. Presentation attacks can occur during enrolment or identification/verification events. Techniques designed to detect presentation artefacts are generally different from those to counter attacks where natural characteristics are used. Defence against presentation attacks with natural characteristics typically relies on the ability of a biometric system to discriminate between genuine enrolees and attackers based on the differences between their natural biometric characteristics. This ability is characterized by the biometric recognition performance of the system – how well or badly a biometric recognition system executes its required functions. Biometric recognition performance and presentation attack detection have a bearing on the security of biometric systems. Hence, the evaluation of these aspects of performance from a security viewpoint will become important considerations for the procurement of biometric products and systems.

Biometric products and systems share many of the properties of other IT products and systems which are amenable to security evaluation using the ISO/IEC 15408 series and ISO/IEC 18045 in the standard way. However, biometric systems embody certain functionality that needs specialized evaluation criteria and methodology which is not addressed by the ISO/IEC 15408 series and ISO/IEC 18045. Mainly, these relate to the evaluation of biometric recognition and presentation attack detection. These are the functions addressed in ISO/IEC 19989 (all parts).

ISO/IEC 19792 describes these biometric-specific aspects and specifies principles to be considered during the security evaluation of biometric systems. However, it does not specify the concrete criteria and methodology that are needed for security evaluation based on the ISO/IEC 15408 series.

The ISO/IEC 19989 series provides a bridge between the evaluation principles for biometric products and systems defined in ISO/IEC 19792 and the criteria and methodology requirements for security evaluation based on the ISO/IEC 15408 series. The ISO/IEC 19989 series supplements the ISO/IEC 15408 series and ISO/IEC 18045 by providing extended security functional requirements together with assurance activities related to these requirements. The extensions to the requirements and assurance activities found in the ISO/IEC 15408 series and ISO/IEC 18045 relate to the evaluation of biometric recognition and presentation attack detection which are particular to biometric systems.

ISO/IEC 19989-1 consists of the introduction of the general framework for the security evaluation of biometric systems, including extended security functional components, and supplementary methodology, which is additional evaluation activities for the evaluator. The detailed recommendations are developed for biometric recognition performance aspects in this document and for presentation attack detection aspects in ISO/IEC 19989-3.

This document describes supplements to the evaluation methodology for biometric recognition performance evaluation for the security evaluation of biometric products. It supplements the ISO/IEC 15408 series, ISO/IEC 18045 and ISO/IEC 19989-1. It builds on the general considerations described in ISO/IEC 19792 and the biometric performance testing methodology described in ISO/IEC 19795-1 by providing additional guidance to an evaluator.

In this document the term “data subject” is used while "user" is used in ISO/IEC 19989-1, in order to be consistent with biometric vocabulary, as biometric experts are supposed to be the main readers of this document.

Information security — Criteria and methodology for security evaluation of biometric systems —

Part 2: Biometric recognition performance

1 Scope

For security evaluation of biometric verification systems and biometric identification systems, this document is dedicated to the security evaluation of biometric recognition performance applying the ISO/IEC 15408 series.

It provides requirements and recommendations to the developer and the evaluator for the supplementary activities on biometric recognition performance specified in ISO/IEC 19989-1.

The evaluation of presentation attack detection techniques is out of the scope of this document except for presentation from impostor attempts under the policy of the intended use following the TOE guidance documentation.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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 2382:2015, *Information technology — Vocabulary*

ISO/IEC 2382-37:2017, *Information technology — Vocabulary — Part 37: Biometrics*

ISO/IEC 15408-1:2009, *Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model*

ISO/IEC 15408-3:2008, *Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components*

ISO/IEC 18045:2008, *Information technology — Security techniques — Methodology for IT security evaluation*

ISO/IEC 19792:2009, *Information technology — Security techniques — Security evaluation of biometrics*

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

ISO/IEC 19795-2:2007, *Information technology — Biometric performance testing and reporting — Part 2: Testing methodologies for technology and scenario evaluation*

ISO/IEC 19989-1:2020, *Information security — Criteria and methodology for security evaluation of biometric systems — Part 1: Framework*

ISO/IEC 30107-3:2017, *Information technology — Biometric presentation attack detection — Part 3: Testing and reporting*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 2382-37:2017, ISO/IEC 2382:2015, ISO/IEC 15408-1:2009, ISO/IEC 18045:2008, ISO/IEC 30107-3:2017 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1
bona fide presentation
interaction of the biometric capture subject and the biometric data capture subsystem in the fashion intended by the policy of the biometric system

Note 1 to entry: Bona fide is analogous to normal or routine, when referring to a bona fide presentation.

Note 2 to entry: Bona fide presentations can include those in which the user has a low level of training or skill. Bona fide presentations encompass the totality of good-faith presentations to a biometric data capture subsystem.

Note 3 to entry: The concept "in the fashion intended by the policy of the biometric system" for bona fide is included in the concept "in accordance with the policy of the intended use of the biometric system" used in this document

[SOURCE: ISO/IEC 30107-3: 2017, 3.1.2, modified — Note 3 to entry has been added]

3.2
bona fide presentation classification error rate
BPCER
proportion of bona fide presentations incorrectly classified as presentation attacks in a specific scenario

[SOURCE: ISO/IEC 30107-3: 2017, 3.2.2]

3.3
detection error trade-off curve
DET curve
modified ROC curve which plots error rates on both axes (false positives on the x-axis and false negatives on the y-axis)

Note 1 to entry: An example set of DET curves is shown in ISO/IEC 19795-1:2006, Figure 3.

[SOURCE: ISO/IEC 19795-1:2006, 4.7.1]

3.4
false accept rate
FAR
proportion of verification transactions with wrongful claims of identity that are incorrectly confirmed

[SOURCE: ISO/IEC 19795-1:2006, 4.6.6]

3.5
false-negative identification-error rate
FNIR
proportion of identification transactions by users enrolled in the system in which the user's correct identifier is not among those returned

[SOURCE: ISO/IEC 19795-1:2006, 4.6.8]

3.6
false-positive identification-error rate
FPIR
proportion of identification transactions by users not enrolled in the system, where an identifier is returned

[SOURCE: ISO/IEC 19795-1:2006, 4.6.9]

3.7
false reject rate
FRR
proportion of verification transactions with truthful claims of identity that are incorrectly denied

[SOURCE: ISO/IEC 19795-1:2006, 4.6.5]

3.8
impostor attack presentation match rate
IAPMR
<full-system evaluation of a verification system> proportion of impostor attack presentations using the same PAI species in which the target reference is matched

[SOURCE: ISO/IEC 30107-3: 2017, 3.2.6]

3.9
operating point
setting of a biometric system to operate at a fixed decision threshold

Note 1 to entry: An operating point can be directly represented by a decision threshold or can be represented by a predefined configuration parameter.

3.10
policy of the intended use
policy stating how bona fide presentations are to be made

Note 1 to entry: Intended use is about how natural biometrics should be used with the TOE, i.e. presentations made in the way that bona-fide presentations are made. Presentations made with artefacts are not considered.

4 Abbreviated terms

ATE	assurance class tests
AVA	assurance class vulnerability assessment
FAR	false accept rate
FMR	false match rate
FNIR	false-negative identification-error rate
FNMR	false non-match rate
FPIR	false-positive identification-error rate
FRR	false reject rate
FTAR	failure to acquire rate
FTER	failure to enrol rate
IT	information technology

PAD	presentation attack detection
PAI	presentation attack instrument
PP	protection profile
ST	security target
TOE	target of evaluation
TSF	TOE security functionality

5 Supplementary activities to ISO/IEC 18045 on ATE tests

5.1 General

5.1.1 Guidance

Clause 5 contains guidance, additional requirements and supplements to evaluation activities from ISO/IEC 19989-1:2020, Clause 14, for the evaluator.

The definition of authentication can be found in ISO/IEC 2382.

The definitions of biometric (adjective), biometric capture, biometric capture device, biometric characteristic, biometric enrolee, biometric enrolment, biometric enrolment database, biometric feature, biometric identification, biometric impostor, biometric presentation, biometric recognition, biometric reference, biometric sample, biometric system, biometric verification, comparison, enrol, failure-to-acquire rate, failure-to-enrol rate, false match rate, false non-match rate, match and threshold can be found in ISO/IEC 2382-37.

NOTE 1 In this document, the expression "capture device" is sometimes used instead of “biometric capture device”.

NOTE 2 In this document, the short expression “enrolee” is used instead of “biometric enrolee”.

NOTE 3 In this document, the short expression “enrolment” is used instead of “biometric enrolment”.

NOTE 4 In this document, the short expression “feature” is often used instead of “biometric feature”.

NOTE 5 In this document, the expression "impostor" is sometimes used instead of “biometric impostor”.

NOTE 6 In this document, the short expression “presentation” is often used instead of “biometric presentation”.

The definitions of assurance, attack potential, class, component, confirm, describe, determine, developer, development, ensure, evaluation, guidance documentation, identity, interaction, interface, object, operation, operational environment, potential vulnerability, protection profile, security target, target of evaluation, TOE security functionality, verify and vulnerability can be found in ISO/IEC 15408-1.

NOTE 7 The term "operation" is related to the AGD class.

The definitions of check, examine, methodology and report can be found in ISO/IEC 18045.

The definitions of presentation attack, presentation attack detection and presentation attack instrument can be found in ISO/IEC 30107-1.

Biometric systems employ technology and functionality that require special considerations when conducting security evaluation, including security evaluation based on the ISO/IEC 15408 series. One of these is the non-deterministic nature of biometric decisions, i.e. match; non-match; and other decisions, and the consequent possibility of decision errors (e.g. false match, false non-match) which can have security implications for biometric systems.

A test of the security relevant biometric recognition error rates is an important aspect of every security evaluation of a biometric system. Further, the requirements in ISO/IEC 19989-1 ensure that also the developer of the biometric system under evaluation shall test the error rates of the system under the policy of the intended use following the TOE guidance document.

NOTE 2 In this document, the intended use following the TOE guidance document covers both genuine and imposter attempts, as long as the usage is consistent with the guidance. The guidance is provided by the TOE developer.

This clause contains guidance and additional requirements for the evaluator and review of the developer tests as well as for planning, conducting and reporting independent testing of the error rates of the biometric system. This clause may also be used by the developer of a biometric system to be informed about the requirements.

NOTE 3 In this document, the evaluator is considered competent under the framework of evaluations under ISO/IEC 15408 (all parts) and in particular ISO/IEC 15408-1.

Subclauses 5.1 to 5.4 are applicable to both ATE_IND and ATE_FUN. Subclause 5.5 is specific to ATE_FUN, related to functional tests. Subclause 5.6 introduces the specific aspects resulting from ISO/IEC 19989-1. Subclause 5.7 is for ATE_IND.2 part related to developer tests. Subclause 5.8 is specific to independent testing.

The evaluator should, as a default principle, follow the recommendations introduced thereafter (e.g. on error rates, maximum values, developer testing methodology, etc.). If the evaluator judges they are not appropriately chosen with respect to the TOE and the application, they may use more appropriate values for testing and shall provide justification for the choice of values in the evaluation report. The technology specific aspects in this clause have been developed under consideration of the requirements in ISO/IEC 19795-1. The type of testing to be performed (scenario, technology or operational testing) shall be determined by the evaluator, based on the nature of the TOE and the TOE security target (see 5.1.3 for further information).

In addition to the requirements and recommendations provided in this clause, the evaluator shall also follow the requirements for the assurance components selected by the TOE for the ATE class in ISO/IEC 15408-3 and shall follow the requirements of the corresponding activities in ISO/IEC 18045.

The configuration of the TOE can have an effect on the biometric recognition performance. Hence, the evaluator shall ensure that the TOE configuration for testing complies with the requirements specified in the ST or PP. In particular, when the TOE includes PAD functionality, the evaluator shall check that the PAD functionality is enabled and correctly configured while conducting the biometric recognition performance testing. If both biometric recognition performance and PAD are evaluated for the TOE, the bona fide presentation classification error rate (BPCER) as defined in ISO/IEC 30107-3 should be calculated in biometric recognition performance testing, by additionally recording the output of the PAD subsystem as a supplementary information in the documentation for the ATE_FUN activity of the PAD evaluation. Similarly, the impostor attack presentation match rate (IAPMR) as defined in ISO/IEC 30107-3 may be retrieved from the ATE_FUN activity of the PAD evaluation and taken in account, as it is related to biometric performance.

NOTE 4 The information on IAPMR from PAD evaluation is not useful for the evaluator for estimating FMR/FAR, as those metrics are not directly related. Nevertheless, IAPMR can be a useful information for the evaluator to understand specific behaviours of the recognition algorithms (and it can also be useful for AVA to identify potential weaknesses).

NOTE 5 ATE is focused on validating the performance of the TOE by testing under the policy of the intended use following the TOE guidance document. It therefore encompasses bona fide presentation attempts (as opposed to presentation attacks considered in ISO/IEC 19989-3) for both mated-comparison trials and non-mated comparison trials (i.e. imposter attempts). In both trials, the evaluator can assume use of the TOE in accordance with the policy of the intended use. All other kinds of presentations are considered in ISO/IEC 19989-3.

5.1.2 Remarks for performance evaluation

The relationship between the two error rates FAR/FRR can be illustrated using a detection error trade-off (DET) curve showing the dependency between the two biometric error rates as the decision threshold is varied over its working range (see ISO/IEC 19795-1 for more information). DET curves can be useful to compare the recognition performance of biometric systems and to track improvements in a biometric system over its development. In the context of the evaluation, the biometric system is instead usually considered at only one or a very limited set of decision thresholds.

The developer shall specify the operating point or points of the TOE in the security target, in order to ensure that customer of the TOE is informed about the evaluated configuration.

The evaluator shall ensure that the relevant security settings (including at least the operating points) of the TOE used during performance testing are set, and the evaluation performed in accordance with the values stated in the security target.

Further, it should be considered that a security evaluation following the ISO/IEC 15408 series is focused on IT-security. Therefore, the security relevant biometric recognition error rates of a biometric system shall be assessed in the context of an evaluation. However, because security can be achieved at the expense of usability, usability-related error rates should also be evaluated. Guidance on identifying relevant error rates is given in 5.1.4.3.

Subclauses 5.1.3 to 5.8 provide more detailed information for the evaluator regarding the review of developer tests, repeating a test subset as outlined in ATE_IND.2 and regarding the independent test as required by ATE_IND.1.

5.1.3 Identification of the type of performance evaluation

According to ISO/IEC 19795-1, three basic types of evaluation for the performance rates of a biometric system can be distinguished:

— technology evaluation: off-line evaluation of one or more algorithms for the same biometric modality using a pre-existing or specially collected corpus of samples;

— scenario evaluation: evaluation in which the end-to-end system performance is determined in a prototype or simulated application using live biometric presentations made by a test crew recruited for the test;

— operational evaluation: evaluation in which the performance of a complete biometric system is determined in its operational environment with a specific target population.

The first step for the evaluator is to identify the correct type of the evaluation for the biometric system under evaluation. The type of evaluation shall be determined by the composition of the TOE and what is specified in the security target. The composition of the TOE shall be capable of supporting the specified type(s) of evaluation.

NOTE As evaluations usually refer to an instance of a biometric product rather than to a concrete instance of an installation of a biometric system, the operational test of the security relevant biometric recognition error rates is often not considered. Consequently, most of the content in this clause refers specifically only to technology and scenario cases.

The type of evaluation to be performed depends on the definition of the TOE and the scope in the security target. The evaluator shall verify that the developer testing is appropriate to the type of evaluation.

ISO/IEC 19795-1 further distinguishes between online and offline tests. In online tests, the enrolment or comparison process is executed at the time of image or signal submission while those phases of testing are kept separately in offline tests. Technology evaluations are carried out using offline processing of biometric data. Due to requirements regarding the repeatability and reproducibility that apply to evaluations, pure online tests (in which the images or signals are directly discarded) should not be used.

5.1.4 Biometric recognition error rates

5.1.4.1 Metrics for biometric verification

The class ATE refers in this document to the tests that shall be performed to assess the performance of the biometric system under the policy of the intended use following the TOE guidance document. In the case of a verification biometric system the intended use can be defined as follows: "a data subject tries to be recognized by the system as a legitimate enrolled data subject related to a claimed identity".

In this scenario, the system may anticipate two cases that shall be distinguished: biometric mated comparison trial (i.e. as genuine) and non-mated comparison trial (i.e. as impostor). According to these two cases the following decision error rates shall be reported:

— for an algorithm evaluation, the FMR and FNMR;

— for a system evaluation, the FAR and FRR.

The difference between algorithm error rates (FMR and FNMR) and the system error rates (FAR and FRR) is that the latter depends on the permitted number of verification attempts and may also include other type of errors such as the failure to acquire and failure to enrol.

The FAR (respectively FMR) and FRR (respectively FNMR) error rates of a biometric system are inversely related, the trade-off between the two being determined by the verification decision threshold setting for the system.

Note that other error rate testing that includes the sample acquisition stage typically produces different results for transactions that are limited to a single attempt and those that allow multiple attempts, for example: failure to enrol rate (FTER) and failure to acquire rate (FTAR).

5.1.4.2 Metrics for biometric identification

In an identification scenario, a subject provides a biometric sample without making an explicit claim of identity. The biometric system identifies the subject by biometric comparison of the biometric identification sample with the biometric references of all enrolled subjects until a match is found (or not) based on identification decision criteria defined for the system. This is known as 1:many comparison. Depending on the criteria, zero or more matches can be found and reported by the system. When more than one match is reported, the matching identities can be ranked according to the corresponding comparison scores.

In the case of an identification biometric system, the intended use may be defined as follows:

— positive identification scenario: scenario where the purpose of a biometric system is to verify and identify by means of biometric recognition that a data subject is a specific enrolee in the system without requiring a prior claim of identity;

— negative identification scenario: scenario where the purpose of a biometric system is to confirm by means of biometric recognition that an enrolment data subject is not enrolled in the system.

As with the verification scenario, the class ATE activity refers in this document to the tests that shall be performed to assess the performance of the biometric identification system (TOE) under its intended use. Performance testing shall include:

— if positive identification scenario is considered: performance testing for the case of bona fide presentations, i.e. where members of a test crew (or test data) comprising legitimate enrolled data subjects attempt to be identified by the system as themselves, and performance testing for the case of impostor presentations where members of a test crew (or test data) who are not enrolled in the system attempt to be falsely identified by the system as legitimate enrolees using presentations of their natural biometric characteristics;

— if negative identification scenario is considered: performance testing for the case of non-enrollees-related presentations where members of a test crew (or test data) who are not enrolled in the