INTERNATIONAL STANDARD

ISO/IEC 19795-5

First edition
2011-03-01

Information technology — Biometric performance testing and reporting —

Part 5: Access control scenario and grading scheme

Technologies de l'information — Essais et rapports de performance biométriques —

Partie 5: Plan de classement pour évaluation de scénario de contrôle d'accès

Reference number
ISO/IEC 19795-5:2011(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.

COPYRIGHT PROTECTED DOCUMENT

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) 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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national 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 and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 19795-5 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 37, *Biometrics*.

ISO/IEC 19795 consists of the following parts, under the general title *Information technology — Biometric performance testing and reporting*:

- *Part 1: Principles and framework*
- *Part 2: Testing methodologies for technology and scenario evaluation*
- *Part 3: Modality-specific testing* [Technical report]
- *Part 4: Interoperability performance testing*
- *Part 5: Access control scenario and grading scheme*
- *Part 6: Testing methodologies for operational evaluation*
- *Part 7: Testing of on-card biometric comparison algorithms*

Introduction

This part of ISO/IEC 19795 is concerned solely with the scientific "technical performance testing" of biometric systems and subsystems to be used for access control. Technical performance testing seeks to determine error rates and transaction times with the goal of understanding and predicting the real-world error and transaction times of a biometric system. The error rates include false accept rate, and false reject rate, as well as failure to enrol (FTE) and failure to acquire (FTA) rates across the test population. These measures are generally applicable to all access control systems that contain a biometric verification subsystem.

This part of ISO/IEC 19795 defines a testing framework with the following fundamental aspects.

- This part of ISO/IEC 19795 was conceived to be a framework for a general- or multi-purpose test: "one size fits many (but not all)". The focus is limited to access control applications.
- The framework is suitable as both a requirements statement and an evaluation report.
- The general-purpose nature of this part of ISO/IEC 19795 is centred on the common access control application requirements, and acknowledges the fact that this framework will not be suitable for specialized applications (very high levels of protection, specialized user populations like the elderly, students, etc.). Specialized applications will warrant specialized testing processes.
- The perceived benefit of the general- or multi-purpose test is economy. The supplier can submit to one testing process, and many potential customers can utilize the results, interpreting the suitability of the device (based on the results) for their application.

This testing framework assigns grades representing the tested level of performance, and these grades include a statistical confidence taking the conservative approach, that is, the performance of the system is at least as good as the grade indicated (at the 90% confidence level). Using the grading scheme to specify a required performance level of a system needs to take into account this conservative approach.

It is acknowledged that technical performance testing is only one form of biometric testing. Other types of testing not considered in this part of ISO/IEC 19795 include the following:

- reliability, availability and maintainability;
- security, including vulnerability;
- human factors, including user acceptance;
- environmental;
- safety;
- cost/benefit;
- privacy regulation compliance.

Methods and philosophies for these other types of tests are currently being considered internationally by a broad range of groups.

The purpose of this part of ISO/IEC 19795 is to capture the current understanding by the biometrics community of requirements and best scientific practices for conducting performance testing towards the end of providing consistent, structured evaluations of biometric systems intended for use in access control applications. The framework defined in this part of ISO/IEC 19795 has utility as a method for defining user requirements, for specifying the extent of performance evaluation, for conducting and for reporting.

Information technology — Biometric performance testing and reporting —

Part 5: Access control scenario and grading scheme

1 Scope

This part of ISO/IEC 19795:

- defines a common biometric access control scenario for use in scenario evaluation of biometric verification systems;
- provides a grading scheme for expressing quantitative biometric system requirements and performance levels;
- provides a common basis for conducting scenario evaluations to demonstrate that specified performance grades are being achieved which is adaptable to particular testing facilities and to specific biometric systems.

This part of ISO/IEC 19795 is applicable to performance testing of biometric systems without detailed knowledge of the comparison algorithms or of the underlying distribution of biometric characteristics in the population of interest.

The minimum false accept rate (FAR) tested by this part of ISO/IEC 19795 is 0.1%. If a lower FAR is required, customized testing (outside the scope of this part of ISO/IEC 19795) might be appropriate, and needs to be fully compliant with ISO/IEC 19795-2.

This part of ISO/IEC 19795 addresses testing a biometric system for physical access control, and the suitability of the testing for logical access devices needs to be determined on a case-by-case basis.

Not within the scope of this part of ISO/IEC 19795 is the measurement of error and throughput rates for people deliberately trying to circumvent correct recognition by the biometric system (i.e. active impostors). In addition, this part of ISO/IEC 19795 does not assess the following:

- reliability, availability and maintainability;
- security, including vulnerability;
- human factors, including user acceptance;
- environmental impacts;
- safety;
- cost/benefit/suitability;
- privacy regulation compliance.

These assessments are the responsibility of the procuring authority.

2 Conformance

A test conforms to this part of ISO/IEC 19795 if the scenario used (including test crew demographics, environmental controls, time separation between enrolment and revisit, numbers of attempts and transactions), test conduct, and test reporting all conform to the mandatory requirements in Clauses 5 through 7.

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, *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 TR 19795-3, *Information technology — Biometric performance testing and reporting — Part 3: Modality-specific testing*

4 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 19795-1 and the following apply.

4.1
access control system
ACS
entire electro-mechanical suite that performs the granting or denying of access at controlled entry points of a facility

4.2
biometric subsystem
portion of a biometric system that is present at each access entry point, including the biometric sensor or sampling subsystem

4.3
grade levels
measurement associated with the quantified levels of biometric subsystem performance

NOTE Grade levels are defined, ranging from 0 to 3, or 0 to 6. It is possible that additional grade levels above these values will be defined at a future date.

4.4
FAR level
scale for the relative level of resistance to false accepts in a form associated with three specific false accept rate (FAR) values

4.5
transaction time
time required for the biometric system portion of an access control transaction

NOTE Transaction time is measured in seconds.

5 Definition of testing scenario

5.1 Overview

The goal of testing and evaluating biometric access control systems against the standard set of criteria documented in this part of ISO/IEC 19795 is to ensure that the technical performance of every biometric access control system is evaluated fairly, accurately and equivalently.

Testing shall be performed in a consistent, unbiased manner under conditions that are well understood and documented. Test controls shall be applied to ensure reproducible test results to the most practical extent possible (considering the involvement of human crew members). To accomplish this, every candidate biometric access control system shall be tested in accordance with the same general test protocol.

The procedures to be used shall be based upon a “framework” consisting of specific metrics extracted from biometric system operations and accompanying evaluation criteria which provides for graded evaluation against different levels of false accept rate. The evaluation framework shall accommodate biometric subsystems that output similarity scores or that output only the final match/no match decision.

NOTE 1 Throughout this part of ISO/IEC 19795, where reference is made to similarity scores, it should be understood that for those test results in the form of decision output, the equivalent, suitable process is applied.

NOTE 2 Throughout this part of ISO/IEC 19795, where reference is made to similarity scores, it should be understood that devices that generate dissimilarity scores will be accommodated by making the appropriate threshold comparison matching decisions.

To facilitate the testing of a specific biometric access control system, a specialized biometric test procedure shall be developed. It shall be identical to the general procedure with the exception that any additional information (for example sliding the cover to allow placement of a finger to a sensor) needed in the real-world operation of a particular biometric access control system shall be identified.

5.2 Relationship of biometric system / subsystem to access control system

A biometric access control system is an access control system that contains a biometric system as a subsystem. This biometric system can be, for instance:

- a verification or identification system with centralized biometric template storage;
- a verification system with decentralized biometric template storage in the biometric subsystem; or
- a verification system with localized biometric template storage (e.g. on an ID card).

NOTE 1 The evaluation of identification performance metrics is outside the scope of this part of ISO/IEC 19795.

Figure 1 illustrates the components and information flows in a generic access control system that includes a biometric system. Following Figure 1 is a key to the circled letters representing information flows. Real deployed systems may vary from this general model.

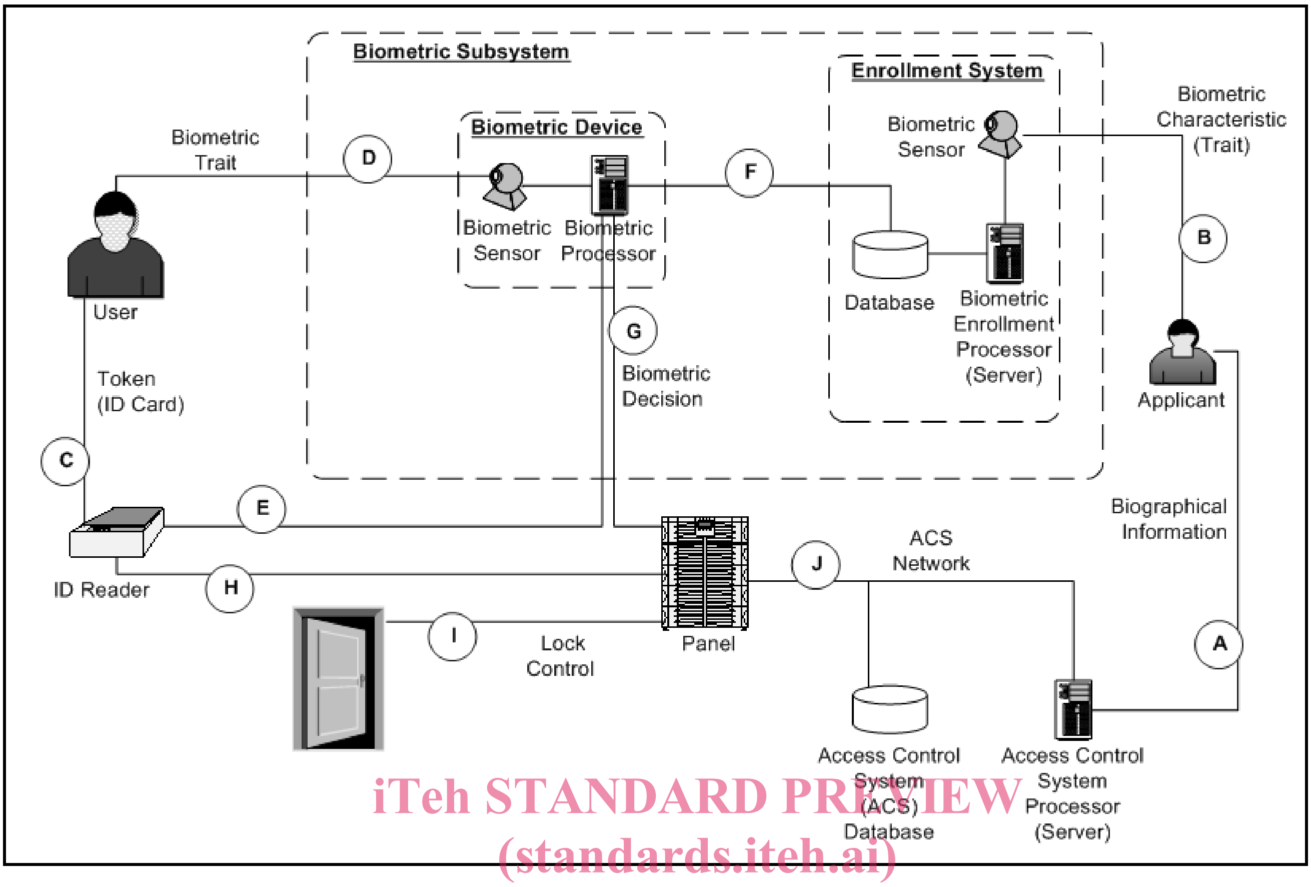

Figure 1 — Generic Biometric Access Control System

A description of the information flow in Figure 1 is as follows:

A. Biographical information: applicant-supplied information (name, address, etc.) obtained during Access Control System (ACS) enrolment via the ACS Processor. This flow is part of a typical legacy ACS.

B. Biometric characteristic (trait): the body part or human behaviour presented by the applicant to the biometric sensor during enrolment (e.g. fingerprint, iris, voice, signature). This flow may also include any interactions between applicant and sensor such as indicator lights or audio feedback.

NOTE 2 An applicant becomes a user only after the enrolment process is completed and access privileges are granted by the access control authority.

C. Token (ID card): any form of machine-readable credential presented by the user to the ID reader to claim an identity.

D. Biometric trait: the body part or human behaviour presented by the user to the biometric sensor during an access transaction (e.g., fingerprint, iris, voice, or signature). This flow may also include any interactions between user and sensor such as indicator lights or audio feedback.

E. User identity code: (ID number, card number, ACS ID) read from the token by the ID reader and sent to the biometric processor as the claim of identity. This flow also includes user template data for template on card architectures.

F. Biometric template data: from enrolment database to biometric processor (for implementations using server-stored templates). This flow is architecture-specific, may be per user transaction or periodic pre-loads.

G. Biometric decision: Yes/No indication (electrical signal or message) from biometric processor to panel conveying the result of the user verification transaction.

H. User identity code: (ID number, card number, ACS ID) read from the token by the ID reader and sent to the panel for the ACS to determine access privilege. This flow is part of a typical legacy ACS.

I. Lock control: electrical signal from the panel used to command the door electro-mechanical locking mechanisms. This flow may also include other signals such as door-open indicators, emergency lock override, etc. This flow is part of a typical legacy ACS.

J. ACS network data: (physical) communication channel (Ethernet, RS485, etc.) enabling data interchange between the panel, ACS processor, and ACS database. The ACS network (logically) depends upon site-specific implementation, and includes a user identity code from panel and user access authorization from ACS processor.

5.3 Evaluation metrics overview

The framework is based on the necessary and sufficient metrics for evaluation of a biometric system for use in an access control application. These metrics are:

- (Single-attempt) false reject rates (FRR_1) at specific values of FAR;
- (Transaction-level) false reject rates (FRR) at specific values of FAR;
- failure to enrol rate (FTE);
- verification transaction time.

To serve many (not all) applications, a range of protection levels, expressed as specific values of FAR, shall be used in this framework.

For each metric, the framework establishes a quantitative grading scheme, using numerical grades, ranging from 0 to 3 (or 0 to 6 for FRR), where a higher score shall indicate better performance and a lower score shall indicate poorer performance. In Clause 7, the metrics are fully defined and the quantitative grading values are established.

NOTE 1 Different metrics may have different grading, as it can be seen in the examples shown in 7.1.5.2 or 7.1.5.3.

NOTE 2 In the kind of test under the scope of this part of ISO/IEC 19795, is not always possible to isolate failure to acquire rate (FTA) cases from false non-match rate (FNMR). Therefore, for the purpose of this part of ISO/IEC 19795, FRR and FRR_1 always include FTA. In case FTA can be obtained, evaluators are encouraged to detail FTA results in the evaluation report.

5.4 Evaluation approach

5.4.1 Tests

The testing defined in this part of the standard shall be Scenario testing under controlled, indoor conditions. The test consists of determination of failure to enrol rate (FTE), verification time, and matching error rates at the single-attempt and transaction levels. The test consists of 10 specific graded metrics: transaction level error rates at three different levels of FAR, attempt level error rates at three different levels of FAR, determination of FTE, and verification transaction time at three different levels of FAR.

A system may, based on supplier request, undergo additional optional testing beyond the graded test. Optional testing designed to generate additional metrics may be conducted depending on the method of operation of the specific system. Such optional testing is not defined by this part of ISO/IEC 19795.

5.4.2 Universality of the test

The rationale for using grade levels versus pass/fail relates to the "universality" or variety of user applications of the evaluation results. Each application is expected to have its own set of required metric grades. A pass/fail evaluation of a system against any particular set of metrics could be developed. However, the introduction of a grade level-based evaluation may provide several advantages. First, a standard test can be defined and used for several different applications. More importantly, the results of a single evaluation can be used by all potential users of the system to judge the suitability of the tested system to their specific application. The system supplier could theoretically reduce overall evaluation cost by submitting to one test, which would optimize the test organization's time and resources. The overall cost for a single graded evaluation may be higher, but could apply to a variety of user applications.

5.4.3 Levels of effort and decision policies

The experimenter shall report enrolment and verification levels of effort and decision policies as follows.

Minimum and maximum number of placements, attempts, and transactions required or permitted to enrol may be somewhat dependant on the enrolment subsystem under test. An enrolment subsystem may allow enrolment after one attempt, or may require multiple presentations, attempts, and transactions. Unless otherwise dictated, the following shall apply:

- three enrolment transactions of up to three attempts each shall be allowed (if unable to enrol on the first or second transaction);
- an enrolment transaction shall be defined by the supplier, consistent with their operational enrolment practices. For modalities with multiple instances (e.g. fingers, irises), the enrolment policy may include attempts with a primary instance (e.g. right index finger), and if that attempt fails, then secondary instances may be used to enrol;
- three attempts shall be allowed for each verification transaction.

Minimum and maximum duration permitted or required to enrol within a given enrolment attempt or transaction may be somewhat dependant on the enrolment subsystem under test. A biometric subsystem may terminate an enrolment attempt or transaction after a fixed duration. This may be due to (1) inability to acquire sufficiently distinctive data or (2) inability to sense any biometric data input. Incident (1) means that a biometric subsystem has acquired and processed data but found it lacking; incident (2) means that the data was not acquired and processed. It is not feasible to allow a biometric subsystem to attempt to acquire data indefinitely; therefore for subsystems that do not time out, a time of 45 seconds shall be established as the default time-out.

5.4.4 Controlled Indoor Environment

In order to allow for comparability of test results and establish one scenario that has common features for testing, some environmental conditions shall be specified. The test environment shall be controlled, representative of an indoor/office environment, and within the specification for conditions for the system under test.

NOTE 1 The environment is a factor that can affect biometric system performance. It is out of the scope of this part of ISO/IEC 19795 to analyse its influence, however, some environmental conditions have to be controlled to reach a common basis for obtaining comparable and repeatable test results.

The following environmental conditions shall be controlled for all tests:

- temperature: 22ºC ± 4ºC;
- relative humidity: 40% to 60%.

The other environmental factors to control (e.g. illumination, noise, vibration, etc.) shall be specified by the test organization taking into account the biometric system under test consistent with ISO/IEC TR 19795-3. The test organization shall report on the controlled environmental conditions and values. Any non-controlled conditions considered to have a significant influence on the test shall be reported.

EXAMPLE 1 For an audio-prompted iris recognition system, the experimenter should control as necessary, record and report the following:

- temperature;
- relative humidity;
- presence of natural and artificial lighting, direction and intensity;
- level of noise.

EXAMPLE 2 For a speaker recognition system, the experimenter should record the following:

- temperature;
- relative humidity;
- level of noise.

Required environmental conditions shall be reached before tests are conducted and shall be controlled during enrolment and verification processes with suitable devices. Such conditions shall be recorded and reported.

NOTE 2 Regarding noise, it may be unrealistic to test in near silence, and uncomfortable for the staff to work in the presence of continuous, high background noise.

NOTE 3 Good testing practice is to avoid noisy, distractive activity in the vicinity of a test activity, such as could result from multiple devices being tested together in close proximity.

NOTE 4 The recommended best practice is to suspend testing if out-of-limits environmental conditions are present.

5.5 Crew characteristics and management

5.5.1 Crew demographics

5.5.1.1 General

Demographic characteristics that shall be controlled are the crew age and gender. If other demographic controls are instituted, the controlled parameters, values and results shall be reported.

5.5.1.2 Age

The age distribution of the crew used shall adhere to the ranges of values shown in Table 1.

Table 1 — Age distribution

Age				
<18	18-30	31-50	51-70	>70
0%	25-40%	25-40%	25-40%	0%

NOTE This age distribution does not include younger than 18 or older than 70. If a different age distribution is required, this part of ISO/IEC 19795 is not applicable. ISO/IEC 19795-2 provides more general scenario testing guidance.

5.5.1.3 Gender

The gender distribution of the crew used shall adhere to the ranges of values shown in Table 2.