TECHNICAL SPECIFICATION

ISO/IEC TS 19795-9

First edition
2019-12

Information technology — Biometric performance testing and reporting —

Part 9: Testing on mobile devices

Reference number
ISO/IEC TS 19795-9:2019(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
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 37, *Biometrics*.

A list of all parts in the ISO/IEC 19795 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

The development of a mass-market in connected mobile devices, e.g. smartphones and tablets, has allowed users the convenience of accessing remotely a variety of services which previously needed face-to-face interactions or to have physical access to the service provider's infrastructure.

For some services, convenience should nevertheless remain secondary to the security needs. These services include for example remote payment on commercial websites, banking transactions or certified signing of official documents. To allow these trustful interactions, the need of reliable user authentication is of paramount importance.

One way to certify the user's identity is to implement biometric authentication ability in the device.

It is then important to properly evaluate the accuracy of biometric authentication to ensure that security is strong enough to allow mobile sensible transactions.

Several biometric modalities are widely utilized in consumer-focused mobile devices. Evaluation of biometric performance for all of these modalities should be consistent and follow the same guidelines, methodologies and requirements. Nevertheless, some modality specific considerations should also be addressed when conducting an evaluation. This document provides a general framework usable for all modalities as well as dedicated recommendations when needed.

ISO/IEC 19795-1 describes three types of biometric performance evaluations: technology, scenario and operational evaluations. ISO/IEC TR 30125[1] recommends scenario evaluation as the most proper type of evaluation for testing biometric performance on mobile devices.

A scenario evaluation is an "end-to-end" biometrics evaluation in which the full system is tested with a careful control of the surrounding conditions. However, when applying this type of evaluation to biometric systems working on mobile devices, testing and reporting methods should consider the particularities and constraints of these use cases.

Information technology — Biometric performance testing and reporting —

Part 9:
Testing on mobile devices

1 Scope

This document provides guidance for performance testing of biometrics when this technology is used on mobile devices with local biometric authentication to improve authentication assurance.

This document aims to:

— Provide guidance for affordable and cost-efficient testing and reporting methods for performance assessment at a full system level of biometric systems embedded in mobile devices with offline evaluation of false accept rate (FAR) claims.

— Define modality-specific considerations of these methods.

This document is applicable to:

— verification use cases related to secure transactions.

This document is not applicable to:

— privacy aspects;

— secure authentication from mobile device to server;

— testing and reporting for presentation attack detection (PAD) mechanisms in mobile devices;

— performance testing of biometric sub-systems such as acquisition sub-system or comparison sub-system;

— continuous authentication.

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 2382-37, *Information technology — Vocabulary — Part 37: Biometrics*

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

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

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 2382-37, ISO/IEC 19795-1 and the following apply.

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

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

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

3.1
mobile device
small, compact, handheld, lightweight computing device, typically having a display screen with digitizer input and/or a miniature keyboard

EXAMPLE Laptops, tablet PCs, wearable ICT devices, smartphones, USB gadgets.

3.2
authentication assurance
confidence in the authentication process

3.3
gender
classification as male, female or some other category based on social, cultural or behavioural factors

Note 1 to entry: This is determined through self-declaration or self-presentation and may change over time.

Note 2 to entry: Depending on jurisdiction recognition, this may or may not require assessment by a third party.

3.4
time limit
longest time before a biometric system returns a decision on accept or reject, success or failure to enrol, success or failure to acquire a biometric sample

Note 1 to entry: All decisions returned after time limit are discarded.

Note 2 to entry: Time limit set to 0 means no time limit. All metrics evaluated are reported with the longest time needed by the biometric system to return decisions.

4 General considerations for biometrics on mobile devices

4.1 Biometric authentication process

Currently there are two types of local authentications that can be executed by mobile devices:

— explicit authentication in which the user is aware that a biometric authentication is going to happen and presents voluntarily his/her biometric characteristic to the capture device;

— passive authentication in which the user is authenticated without active effort by the user.

NOTE This document does not cover biometric systems where the user is continuously authenticated by the system in the background.

Therefore, the definition of testing methods and protocols should consider both types of authentications. In particular, the test plan should consider the following aspects:

— what constitutes the biometric capture process;

— how the user should interact with the mobile device during this process;

— which are the policies to manage failure to acquire (FTA) failures.

4.2 Biometric capture sensor

Mobile devices may have two kinds of biometric capture sensors:

— Embedded sensors which are the generic sensors of a mobile device (e.g. front and back cameras, microphone, touchscreen) but that are used for collecting the biometric characteristic during a biometric authentication.

  For some modalities, biometric acquisition may rely on these embedded sensors, which have not been designed and optimized for this task. Image resolution or uncontrolled image post-processing may for example impede the accuracy of biometric algorithms designed for more controlled acquisition.

— Dedicated sensors which are specific sensors for collecting biometric characteristics (i.e. a fingerprint reader).

Even when dedicated sensors are embedded in the device, they need to be coupled with optimized software in order to take into account hardware and ergonomics constraints specific to a mobile use case. These constraints may include, e.g. lower usable area available for fingerprint, closer range acquisition for face recognition.

A full-system evaluation should be carried out including the biometric capture sensor. Where the same or equivalent capturing sensor and the same comparison algorithm is used, evaluation results for one device may be applicable to others.

For this reason, guidelines for the evaluation should include recommendations to decide the most appropriate sensor to use during the evaluation as well as how to expand test reports to include the characteristics of the evaluated sensor as well as its situation on the device. These guidelines should be defined per biometric modality.

4.3 Uncontrolled environment

A full-system evaluation should control the conditions in which testing is going to be carried out. As described in ISO/IEC TR 30125, one of the major issues of mobile devices is the uncontrolled nature of the capture environment and the variability over time. To obtain realistic results, biometric performance should be analysed in numerous conditions. However, it is unfeasible to do it due to time and budget constraints. Testing conditions should be reduced to measure performance in a limited set of conditions.

Therefore, recommendations for selecting the most proper testing conditions and how to report it should be defined for ambient conditions present during the evaluation. Specific recommendations should be defined per biometric modality.

4.4 Challenges in storing references and generating comparison scores

In most current implementations of biometric authentication on mobile devices, the generation and the storage of the biometric references and samples are protected from external access. Devices are not designed to store multiple references and generate comparison scores from the submission of a probe against these references. Some solution is necessary to the problem of comparing one probe against multiple references on mobile devices, where typically only one reference is available, and scores are not accessible. Solutions could include development of test harnesses, of prototype devices, or of alternative operating modes.

A process for validating results from these alternative operating modes against standard operating modes will be required.

4.5 Adaptation of the biometric references

Finally, most biometric solutions implemented in mobile devices are able to adapt the biometric references over time with the aim to reduce the false rejection rates. To assess the improvement over time, the evaluation methodology should emulate this process.

5 Overview of full-system evaluation of mobile devices

5.1 General description

An evaluation of a biometric system shall conform to the requirements and best practices described in ISO/IEC 19795-1. This document considers mobile devices as a "full biometric system": an end-to-end biometric system, covering all the steps from biometric sample acquisition and biometric characteristics extraction to biometric comparison with a biometric reference. A "full biometric system" evaluation encompasses the testing of all process and subsystems in a realistic scenario. As such, an evaluation shall additionally conform with the requirements of ISO/IEC 19795-2:2007, Clauses 1 to 5, 7 and 8, which are relevant for a scenario evaluation of a verification system.

NOTE Some mobile devices allow the enrolment of several users for biometric identification in a small dataset related to low security features, e.g. device unlocking. This document only considers verification use cases related to secure transactions, which can vary depending on the risk, policy and/or legislation that applies to the transaction.

Mobile devices are short lifecycle products, which may have various versions, regular software updates or hardware specifications changes from one market to another or from one production series to another. Several devices from various manufacturers may integrate the same biometric sensors and software provided by a unique biometric system provider. The evaluator shall determine exactly what is the Target of Evaluation (ToE) and what the evaluation covers.

The evaluation of the ToE may be in-house testing performed by the system manufacturer, or a third-party evaluation. The third-party may, for example, be a certification body, whose main objective would be to assess if the ToE meets or exceeds performance requirements relevant for the certification scheme.

EXAMPLE A certification scheme can require that a mobile device has a false reject rate (FRR) below 1 % and a FAR below 0,01 %. The system provider will claim that its product meets the requirements. The evaluator will test the mobile device and determine if observed errors rates support the claim.

For most of the currently commercialized mobile devices with biometric capabilities, the biometric application is a black-box for security and privacy reasons. Biometric samples are stored in a secure environment and all computations occur in a secure execution environment, with no access to biometric data or any intermediate results. A third-party evaluation requires that the system provider delivers a customized version providing access to biometric data or to detailed transaction logs.

5.2 Considerations for time efficient evaluation

5.2.1 Factors that increase the time and cost of biometric performance evaluations

There are different aspects that increase the time and cost of a performance evaluation:

— The minimum error rates to be able to determine with a statistically significant level of confidence. Depending on the expected error rates and the statistical significance to achieve, the number of transactions to perform may increase considerably. This fact entails an increase in either the number of subjects that participate in the evaluation, the number of visits or the number of transactions to be conducted by test subjects.

— The inability to store large amount of biometric data and to get access to the captured biometric samples and/or stored biometric references. As mentioned in the Introduction, mobile devices allow a few biometric references to be saved, and most of the time it is not possible to get access to them

for an external application due to security reasons. Both circumstances increase the time and the cost of the evaluation because testing procedures must be carried out online.

— The number of conditions to evaluate. Mobile devices are used in a diversity of situations (i.e. sitting at a table, standing, walking, or driving) in which the ambient conditions are changing constantly so there are innumerable scenarios for which biometric performance testing should be analysed.

5.2.2 Reduction of the number of recognition transactions

5.2.2.1 Approaches

The main challenge of a biometric evaluation of a mobile device for the evaluator is to assess that the observed errors rates, FAR and FRR, support a claimed performance with a sufficient statistical certainty.

ISO/IEC 19795-1 recommends the use of Rule of 3 or Rule of 30 approaches to assess performance claims.

— Rule of 3 defines the minimum number of transactions required for the estimation of a minimum error rate at a 95 % confidence level when no errors are obtained during the evaluation.

— Rule of 30 states that to be 90 % confident that the true error rate is within ±30 % of the observed error rate, there should be at least 30 errors. Based on the predefined error rates and the number of errors, i.e. 30 errors, it is possible to define the minimum number of transactions.

The target requirement for an error will directly influence the number of independent tests required to have statistical significance, and thus the size of the test crew, the time spent and the cost of the evaluation. To reduce the duration and cost of executing a biometric performance evaluation, the number of recognition transactions can be constrained.

EXAMPLE Evaluating a 0,1 % FAR rate by Rule of 30 requires 30000 independent tests (more precisely, an observed error rate of 0,1 % would mean the true error rate is between 0,07 % and 0,13 % with 90 % confidence). For the same 0,1 % FAR rate, Rule of 3 would only require 3000 independent tests, but the claim is only verified (with 95 % confidence level) if no error is observed, i.e. a test is not conclusive if only one error occurs.

For FAR evaluation, while the independence criteria would require that one test subject is only involved in one impostor transaction, it is commonly agreed that the statistical loss of computing all possible cross-comparisons between test subjects is acceptable. This approximation shall be considered relevant for a mobile device evaluation (i.e. with N test subjects, N*(N-1)/2 impostors tests can be made). Table 1 gives examples of the number of test subjects required for various FAR targets. In general, all possible cross-comparisons can only be executed offline.

Table 1 — Number of tests required in an evaluation for various FAR targets following Rule of 3 or Rule of 30

FAR target	Rule of 3		Rule of 30	
	Minimal number of tests required	Minimal number of test subjects	Minimal number of tests required	Minimal number of test subjects
1 %	300	25	3000	78
0,1 %	3000	78	30000	246
0,01 %	30000	246	300000	776
0,001 %	300000	776	3000000	2450
0,0001 %	3000000	2450	30000000	7747

As noted in 5.1, a third-party evaluation of FAR would quickly be impractical and time consuming if the evaluator only has access to an unmodified mobile device. The main drawback would be the impossibility to enrol more than one person on the mobile device at a time, meaning that each verification transaction must be done separately and that the enrolled person should be changed regularly.