International Standard

ISO/IEC 30107-4

Second edition
2024-02

Information technology — Biometric presentation attack detection —

Part 4: Profile for testing of mobile devices

Technologies de l'information — Détection d'attaque de présentation en biométrie —

Partie 4: Profil pour les essais des dispositifs mobiles

Reference number
ISO/IEC 30107-4:2024(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 37, *Biometrics*.

This second edition cancels and replaces the first edition (ISO/IEC 30107-4:2020), which has been technically revised.

The main changes are as follows:

— removal of terms and definitions present in other parts of the ISO/IEC 30107 series;

— addition of FIDO biometrics requirements;

— addition of Clause 4;

— best practice number of PAI species used in evaluation changed from minimum 3 to minimum 6;

— FIDO biometric presentation attack detection evaluation requirements has been moved to Clause 7;

— removal of Annex A: Roles in PAD testing of mobile devices;

— other minor wording changes to align with ISO/IEC 30107-3.

A list of all parts in the ISO/IEC 30107 series can be found on the ISO and IEC websites.

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

The presentation of an artefact or of human characteristics to a biometric capture subsystem in a fashion intended to interfere with system policy is referred to as presentation attack. The ISO/IEC 30107 series deals with techniques for the automated detection of presentation attacks. These techniques are called presentation attack detection (PAD) mechanisms. ISO/IEC 30107-3 establishes principles and methods for performance assessment of PAD mechanisms and for reporting the results thereof.

PAD mechanisms are commonly integrated into mobile devices that use biometrics.[1][2] The following characteristics of mobile devices necessitate the development of an ISO/IEC 30107-3 profile specific to mobile devices:

— Mobile devices often have accelerated product development timelines, therefore time and resources for PAD testing can potentially be limited.

— A single type of biometric subsystem is often integrated into a wide range of mobile devices, such that results from a single test can be applicable to multiple types of mobile devices with the same operating system (OS) or using the same development language.

— Biometric subsystems integrated into mobile devices are typically closed systems, such that performance testing takes place through a full-system evaluation.

This document provides requirements for assessing the performance of PAD mechanisms on mobile devices with local biometric recognition. A general profile is provided in Clause 5 as well as a profile specific to Fast IDentity Online (FIDO) biometric presentation attack detection evaluation requirements in Clause 6.[3]

Information technology — Biometric presentation attack detection —

Part 4: Profile for testing of mobile devices

1 Scope

This document is a profile that specifies requirements for testing biometric presentation attack detection (PAD) mechanisms on mobile devices with local biometric recognition and on biometric modules integrated into mobile devices.

The profile lists requirements from ISO/IEC 30107-3 that are specific to mobile devices. It also establishes requirements that are not present in ISO/IEC 30107-3. For each requirement, the profile defines an "Approach in PAD Tests for Mobile Devices". For some requirements, numerical values or ranges are provided in the form of best practices.

This profile is applicable to mobile devices that operate as closed systems with no access to internal results, including mobile devices with local biometric recognition as well as biometric modules for mobile devices.

This document is not applicable to mobile devices with solely remote biometric recognition.

The attacks considered in this document take place at the capture device during the presentation and collection of biometric characteristics. Any other attacks are outside the scope of this document.

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 30107-1, *Information technology — Biometric presentation attack detection — Part 1: Framework*

ISO/IEC 30107-3, *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, ISO/IEC 19795-1, ISO/IEC 30107-1, ISO/IEC 30107-3 and the following apply.

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

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

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

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

Note 1 to entry: Examples include laptops, tablet PCs, wearable information and communication technology (ICT) devices, and smartphones

3.2
biometric module
small, compact and lightweight unit that is integrated into or interfaces with a mobile device and that captures biometric samples, compares biometric references or stores biometric templates

4 Abbreviated terms

The abbreviated terms below are used in this document.

FAR	false accept rate
FIDO	Fast IDentity Online
FRR	false reject rate
FS-PD	full system processing duration
IAPAR	impostor attack presentation accept rate
$IAPAR_{AP}$	impostor attack presentation accept rate at the given attack potential
IUT	item under test
OS	operating system
PAD	presentation attack detection
PAI	presentation attack instrument
TOE	target of evaluation

5 Conformance

Evaluations not based on FIDO biometric requirements shall be planned, executed and reported in accordance with all requirements set forth in Clause 6.

Evaluations based on FIDO biometrics requirements shall be planned, executed and reported in accordance with all requirements set forth in Clause 7.

6 General profile for PAD testing of mobile devices

Table 1 provides a profile for PAD testing of mobile devices. Requirements are numbered within Table 1 for ease of reference.

Table 1 — Profile for PAD testing of mobile devices

ISO/IEC 30107-3:2023, clause or subclause no.	Requirement	Approach in presentation attack detection (PAD) testing of mobile devices
6	1) Evaluations of PAD mechanisms and resulting reports shall specify the type of presentation attacker (biometric impostor or biometric concealer) considered in an evaluation.	Presentation attacks for PAD testing of mobile devices are executed by biometric impostors.
6	2) Evaluations of PAD mechanisms and resulting reports shall describe the type of evaluation conducted as well as the attack types to be tested.	The evaluator shall specify one of the following: — Evaluations of PAD mechanisms in which the set or range of attack types is selected to be appropriate to the application, such as those discussed in ISO/IEC 30107-3:2023, Clause 11. — Product-specific evaluations of PAD mechanisms, used to test a supplier's claim of performance against a specific category of attack types.
7.1	3) PAD evaluations and resulting reports shall fully describe the IUT, including all configurations and settings as well as the amount of information available to the evaluator about PAD mechanisms in place.	The evaluator shall provide narrative, to include the following: — Mobile device model, OS, and OS version. — Position of sensor (e.g. front, back, side), to include position relative to device's screen(s). — If applicable, manner of test subject interaction with the biometric sensor (e.g. touch left index finger, swipe right or left thumb, look at front-facing camera, speak a passphrase). — If applicable, the positioning of the biometric module with respect to the mobile device.
7.1	4) Evaluations of PAD mechanisms and resulting reports shall specify the applicable evaluation level, whether PAD subsystem, data capture subsystem, or full system.	PAD testing of mobile devices is applied at the full system level.
7.2	5) Evaluations of PAD mechanisms shall cover a defined variety of attack types by utilizing a representative set of presentation attack instruments and a representative set of bona fide test subjects.	The evaluator shall determine the suitable range of PAIs and bona fide test crew composition.
7.2	6) The evaluator shall define the parameters of the attack presentation to fully characterize the range of PAI presenter interactions with the IUT, to include the temporal boundaries of the presentation.	The evaluator shall provide basis and narrative.
7.2	7) In an evaluation of PAD mechanisms, the evaluator shall 1) define bona fide presentations and representative test subjects for the target application and population and 2) provide a rationale for these definitions.	The evaluator shall provide basis and narrative.
10.2	8) Evaluations of PAD mechanisms and resulting reports shall describe how artefacts were created and prepared, addressing the following:	The evaluator shall provide basis and narrative for each bullet.

Table 1 *(continued)*

ISO/IEC 30107-3:2023, clause or subclause no.	Requirement	Approach in presentation attack detection (PAD) testing of mobile devices
	— creation and preparation processes; — effort required to create and prepare artefacts (e.g. technical know-how, creation time, difficulty of collecting artefact materials, creation instruments, and preparation instruments); — ability to consistently create and prepare artefacts with intended properties; — customization of artefacts for specific PAI presenters; — customization of artefacts for specific systems; — sourcing of biometric characteristics; — availability of public information on creation and preparation process; — changes in artefact creation or preparation processes over the course of the evaluation.	
10.3	9) Evaluations of PAD mechanisms and resulting reports shall describe how artefacts were used in the evaluation, addressing the following: — level of PAI presenter training and habituation; — artefact durability, including the number of presentations associated with each artefact; and — level of scrutiny or oversight applied during artefact usage.	The evaluator shall provide basis and narrative for each bullet. It is assumed that no scrutiny or oversight is applied during artefact usage.
11.1	10) Evaluations of PAD mechanisms and resulting reports shall describe whether evaluation design considered enrolment, identification, and/or verification processes	The evaluator shall document which processes were considered in evaluation design: enrolment, verification, or identification.

Table 1 *(continued)*

ISO/IEC 30107-3:2023, clause or subclause no.	Requirement	Approach in presentation attack detection (PAD) testing of mobile devices
11.2	11) Evaluations of PAD mechanisms and resulting reports that apply to enrolment processes shall describe the following: — use of enrolment-specific quality thresholds or presentation policy; — parameters of the enrolment transaction, including number and duration of presentations; — level of operator oversight present in the process; — manner in which operator functions were applied or emulated in the evaluation; and — whether the IUT checks sample quality and provides feedback to the test subject (e.g. “finger too wet”, “move to a quieter room”).	The evaluator shall provide basis and narrative for each bullet. Assumptions for enrolment processes include the following: — enrolment parameters are native to the device and are not changeable or exposed to the evaluator; — no operator oversight is present; and — no operator functions are applied or emulated in the evaluation.
11.3	12) Evaluations of PAD mechanisms and resulting reports that apply to verification processes shall describe the following: — use of quality thresholds and presentation policy; — parameters of the verification transaction, including the number and duration of presentations; — level of operator oversight present in the process;	The evaluator shall provide basis and narrative for each bullet. Assumptions for verification processes include the following: — verification parameters are native to the device and not changeable or exposed to the evaluator; — no operator oversight is present in the process; and — no operator functions are applied or emulated in the evaluation.

Table 1 *(continued)*

ISO/IEC 30107-3:2023, clause or subclause no.	Requirement	Approach in presentation attack detection (PAD) testing of mobile devices
	— manner in which operator functions were applied or emulated in the evaluation; — whether the IUT checks sample quality and provides feedback to the test subject (e.g. “finger too wet”, “move to a quieter room”); — policy after failing all attempts, e.g. asking for a PIN, a password, or waiting for 30 s before attempting again; — whether the IUT provides feedback after a failed attempt; and — if the IUT provides feedback, a list of the feedback messages.	Transaction policies, attempt limits, and user feedback are particularly important when considering mobile devices and shall be documented thoroughly and accurately. Policies that lead to user revocation and/or device locking after a number of failed attempts can make an evaluation impractical. Special evaluation settings allowing sequences of multiple failed transactions can be requested of the device manufacturer to allow an efficient evaluation. Test device OS settings shall not interfere with transaction policies (such as timing out/locking screen based upon a time limit) that are being evaluated. NOTE 1 The behaviour of the IUT after failed transactions can also influence attack approaches. Feedback provided by the IUT can influence IAPAR, as PAI presenters can improve their attack presentations by adapting the artefact creation process in response to feedback. EXAMPLE 1 Feedback provided by the mobile device can include the following: **Modality** / **Feedback from mobile device** Fingerprint / “Finger too wet” Fingerprint / “Make sure that your finger covers the entire Home button” Face / “Look at the camera” Voice / “Move to quieter place”

Table 1 *(continued)*

ISO/IEC 30107-3:2023, clause or subclause no.	Requirement	Approach in presentation attack detection (PAD) testing of mobile devices
13.1	13) Evaluations of PAD mechanisms shall report the following:	The evaluator shall provide basis and narrative for each bullet.
	— 14) number of presentation attack instruments used in the evaluation;	The evaluator shall document this number based on IUTs, PAI sources, PAI presenters, species, and series.
	— 15) number of PAI species used in the evaluation;	Best practice is to use at least six PAI species. When a PAD evaluation considers attack potential, then best practice is to use at least six PAI species at each level. NOTE 2 PAD testing designed to assess susceptibility to a broader range of attacks would require that more PAI species be used. NOTE 3 If the test is meant to demonstrate resistance to attackers with a certain level of attack potential in a grading scheme, best practice is to use at least six PAI species for each and any level of attack potential below the level that resistance is claimed to, in addition to at least six PAI species at that level of attack potential.
	— 16) number of PAI series used in the evaluation;	If an attack using a PAI species does not reproducibly succeed using less than 10 PAI series, best practice is to use at least 10 PAI series. NOTE 4 Certain evaluations will possibly need to take place with fewer than 10 PAI series, such as evaluations utilizing expensive, high-quality masks.
	— 17) number of individuals involved in the testing, including PAI presenters unable to utilize artefacts and test subjects unable to present non-conformant characteristics; — 18) number of sources from whom or which artefact characteristics were derived;	The evaluator shall provide basis and narrative for each bullet.
	— 19) number of artefacts created per PAI source for each PAI species;	Best practice is to create a minimum of three PAIs per PAI source for each species. NOTE 5 This is equivalent to the length of a PAI series. NOTE 6 PAD testing not concerned with repeatability of PAIs can allow for fewer PAIs to be created per species and PAI source.
	— 20) number of tested materials;	The evaluator shall provide basis and narrative.
	— 21) description of output information available from PAD mechanism;	The evaluator shall provide basis and narrative, based on native system operations.
	— 22) ordering of presentations with and without PAIs, and whether PAI presenters or test subjects were reused;	The evaluator shall provide basis and narrative.

Table 1 *(continued)*

ISO/IEC 30107-3:2023, clause or subclause no.	Requirement	Approach in presentation attack detection (PAD) testing of mobile devices
	— 23) ordering of presentations to the PAD enabled and disabled system, and whether test subjects were reused.	The evaluator shall provide basis and narrative.
	24) The experimenter shall, in the test report: — define the purpose and responsibilities of the following roles in a PAD test: test subject (conducts bona fide presentations and non-conformant capture attempts), PAI presenter, PAI source, and PAI creator; — state whether the role was material to test results and provide a basis for this assertion; — indicate the number of individuals who occupied each role (e.g. five individuals were PAD sources in the test); — for each role, describe individuals' level of experience with presentation attacks; — document occurrences in which individuals occupied multiple roles, e.g. PAI sources were also PAI presenters.	The evaluator shall provide basis and narrative for each bullet.
	25) For a full-system evaluation of impostor attacks, the PAI presenter shall not conduct presentations in which they are enrolled as a bona fide reference.	The evaluator shall provide basis and narrative.
	26) Test reports shall describe any use of machines or automated mechanisms as PAI presenters or PAI sources.	The evaluator shall provide basis and narrative.
13.4.2.1	27) For a given verification system IUT, for each PAI species, the following shall be reported: — IAPAR and the sample size on which this computed rate is based; — FRR/FAR; — FS-PD (optional). For a given IUT, the IAPAR of the most successful PAI species with attack potential AP may be reported as $IAPAR_{AP}$. For bona fide test subjects, the evaluator shall report FRR/FAR calculations and the basis of results.	The evaluator shall provide results and basis of calculations.

7 FIDO Profile for PAD testing of mobile devices

Table 2 provides a profile for PAD testing of mobile devices based on FIDO biometrics requirements. Requirements are numbered within Table 2 for ease of reference.

Table 2 — Profile for PAD testing of mobile devices for FIDO biometrics requirements

ISO/IEC 30107-3:2023, clause or subclause no.	Requirement	Approach in presentation attack detection (PAD) testing of mobile devices for FIDO biometrics requirements
6	1) Evaluations of PAD mechanisms and resulting reports shall specify the type of presentation attacker – biometric impostor or biometric concealer – considered in an evaluation.	FIDO shall use biometric impostor.
6	2) Evaluations of PAD mechanisms and resulting reports shall describe the type of evaluation conducted as well as the attack types to be tested.	FIDO shall use application-focused evaluations of PAD mechanisms in which the set/range of attack types is selected to be appropriate to the application, such as those discussed in ISO/IEC 30107-3:2023, Clause 11.
7.1	3) PAD evaluations and resulting reports shall fully describe the IUT, including all configurations and settings as well as the amount of information available to the evaluator about PAD mechanisms in place.	FIDO test reports shall provide the required narrative. FIDO evaluated biometric systems shall evaluate IUTs that are full systems. A FIDO evaluated biometric recognition system is not required to be integrated in a mobile device. However, it shall have the complete functionality of a biometric recognition system (capture, enrolment, quality check, PAD, comparison and decision subsystem, etc.). Additionally, the vendor shall provide an allowed integration document which describes allowable changes of the biometric sub-system when integrated into the mobile device. A TOE shall be provided for each allowed integration, e.g. different thickness of glass. The integration manual is provided for reference to the laboratory, it shall be coherent with the configuration and operation of the test harness. While FIDO certifications can be performed in the context of a mobile device, certification is also allowed at a component level. When the biometric module under test is integrated into a mobile device, the evaluator shall provide narrative, including the following:
		— mobile device model, OS, and OS version; — position of sensor (e.g. front, back, side), to include position relative to device's screen(s); — if applicable, manner of test subject interaction with the biometric sensor (e.g. touch left index finger, swipe right or left thumb, look at front-facing camera, speak a passphrase).
7.1	4) Evaluations of PAD mechanisms and resulting reports shall specify the applicable evaluation level, whether PAD subsystem, data capture subsystem, or full system.	FIDO shall evaluate the full system.

Table 2 *(continued)*

ISO/IEC 30107-3:2023, clause or subclause no.	Requirement	Approach in presentation attack detection (PAD) testing of mobile devices for FIDO biometrics requirements
7.2	5) Evaluations of PAD mechanisms shall cover a defined variety of attack types by utilizing a representative set of presentation attack instruments and a representative set of bona fide test subjects.	FIDO establishes bona fide test crew composition and PAI usage parameters.
7.2	6) The evaluator shall define the parameters of the attack presentation to fully characterize the range of PAI presenter interactions with the IUT, to include the temporal boundaries of the presentation.	FIDO establishes parameters to test the range of PAI presenter interactions with the IUT, including temporal boundaries.
7.2	7) In an evaluation of PAD mechanisms, the evaluator shall 1) define bona fide presentations and representative test subjects for the target application and population and 2) provide a rationale for these definitions.	FIDO test evaluator shall provide basis and narrative.
10.2	8) Evaluations of PAD mechanisms and resulting reports shall describe how artefacts were created and prepared, to include:	FIDO evaluations require that the evaluator shall provide basis and narrative for each bullet.
	— creation and preparation processes; — effort required to create and prepare artefacts (e.g. technical know-how, creation time, difficulty of collecting artefact materials, creation instruments, and preparation instruments); — ability to consistently create and prepare artefacts with intended properties; — customization of artefacts for specific PAI presenters; — customization of artefacts for specific systems; — sourcing of biometric characteristics; — availability of public information on creation and preparation process; — changes in artefact creation or preparation processes over the course of the evaluation.	
10.3	9) Evaluations of PAD mechanisms and resulting reports shall describe how artefacts were used in the evaluation: — level of PAI presenter training and habituation; — artefact durability, including the number of presentations associated with each artefact; and — level of scrutiny or oversight applied during artefact usage.	FIDO test evaluator shall provide basis and narrative for each bullet.
11.1	10) Evaluations of PAD mechanisms and resulting reports shall describe whether evaluation design considered enrolment, identification, and/or verification processes.	FIDO shall only evaluate verification processes.

Table 2 *(continued)*

ISO/IEC 30107-3:2023, clause or subclause no.	Requirement	Approach in presentation attack detection (PAD) testing of mobile devices for FIDO biometrics requirements
11.2	11) Evaluations of PAD mechanisms and resulting reports that apply to enrolment processes shall describe the following:	FIDO does not evaluate PAD mechanisms that apply to enrolment – N/A.
	— use of enrolment specific quality thresholds or presentation policy; — parameters of the enrolment transaction, including number and duration of presentations; — level of operator oversight present in the process; — manner in which operator functions were applied or emulated in the evaluation; and — whether the IUT checks sample quality and provides feedback to the test subject (e.g. "finger too wet", "move to a quieter room").	
11.3	12) Evaluations of PAD mechanisms and resulting reports that apply to verification processes shall describe the following: — use of quality thresholds and presentation policy; — parameters of the verification transaction, including the number and duration of presentations; — level of operator oversight present in the process; — manner in which operator functions were applied or emulated in the evaluation; — whether the IUT checks sample quality and provides feedback to the test subject (e.g. "finger too wet"); — policy after failing all attempts, e.g. asking for a PIN, a password, or waiting for 30 seconds before attempting again; — whether the IUT provides feedback after a failed attempt; and — if the IUT provides feedback, a list of the feedback messages.	FIDO test evaluator shall provide basis and narrative for each bullet. FIDO has no concept of quality thresholds or presentation policy that can be configured by an evaluator. FIDO evaluations assume that verification parameters are native to the component/device and not accessible or exposed to the evaluator. FIDO evaluations are conducted without operator guidance, and thus no operator oversight is present in the process, nor are they applied or emulated in the evaluations. Not applicable if testing a biometric component.
13.1	13) Evaluations of PAD mechanisms shall report 14): number of presentation attack instruments used in the evaluation.	FIDO evaluations use 25 sources that provide 12 PAI species for a total of 300 PAI instruments.
13.1	13) Evaluations of PAD mechanisms shall report 15): number of PAI species used in the evaluation.	FIDO biometrics requirements specify use of 14 PAI species.
13.1	13) Evaluations of PAD mechanisms shall report 16) number of PAI series used in the evaluation.	FIDO requires to use 10 PAI series per PAI species.