FINAL
DRAFT

INTERNATIONAL
STANDARD

**ISO/IEC
FDIS
30107-4**

ISO/IEC JTC **1**/SC **37**

Secretariat: **ANSI**

Voting begins on:
2023-11-09

Voting terminates on:
2024-01-04

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 FDIS 30107-4:2023(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 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.

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.

Table 1 *(continued)*

ISO/IEC 30107-3:2023, clause or subclause no.	Requirement	Approach in presentation attack detection (PAD) testing of mobile devices
10.2	8) Evaluations of PAD mechanisms and resulting reports shall describe how artefacts were created and prepared, addressing the following: — 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.	The evaluator shall provide basis and narrative for each bullet.
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.