Accenture
Federal
Services

Update on ISO/IEC 30107 Series Presentation Attack Detection Standards

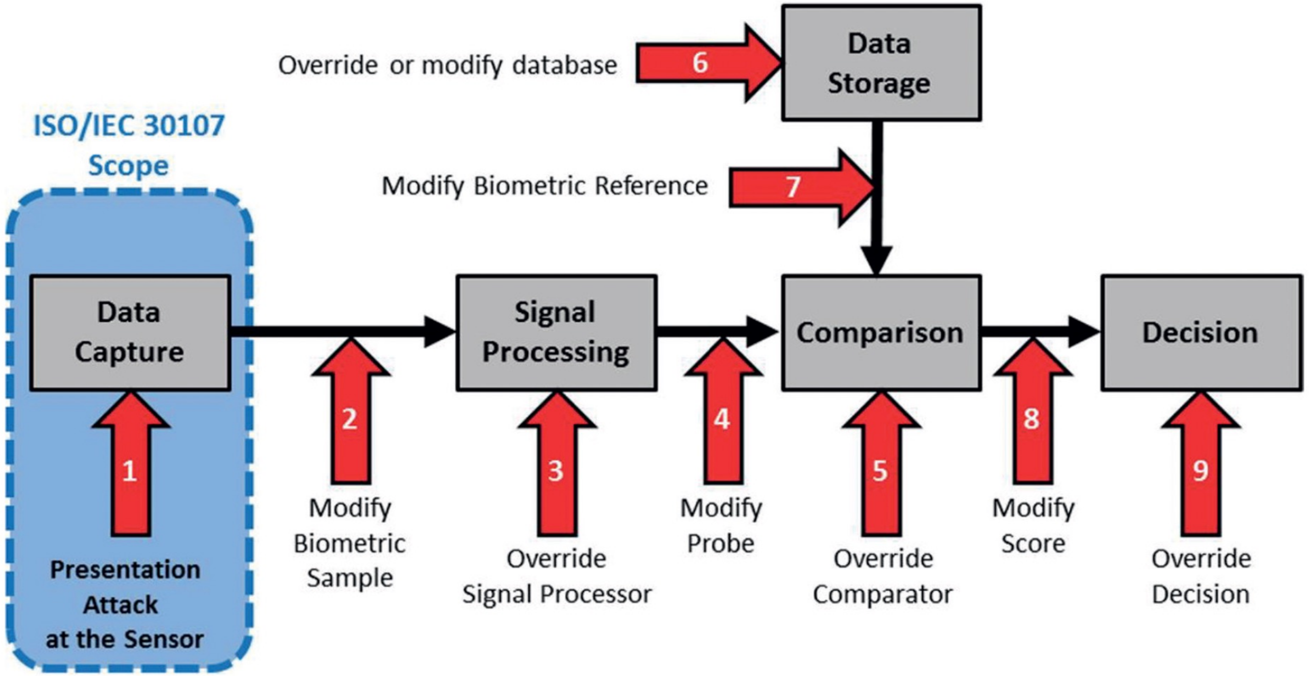
IFPC 2022

Michael Thieme
Managing Director, AFS
michael.thieme@afs.com

Overview of ISO/IEC 30107 Series

- ISO/IEC JTC1 SC 37 Biometrics has published (3) standards and (1) profile on biometric presentation attack detection (PAD)
- (3) documents are under revision to improve alignment and reflect developments in government, industry, and academia

presentation attack detection
automated discrimination between
bona-fide presentations
and biometric presentation attacks



Source: ISO/IEC 30107-1:2016 – Biometric presentation attack detection — Part 1: Framework

Update on ISO/IEC 30107 Series Presentation Attack Detection Standards

ISO/IEC 30107-1:2016 – Biometric presentation attack detection — Part 1: Framework

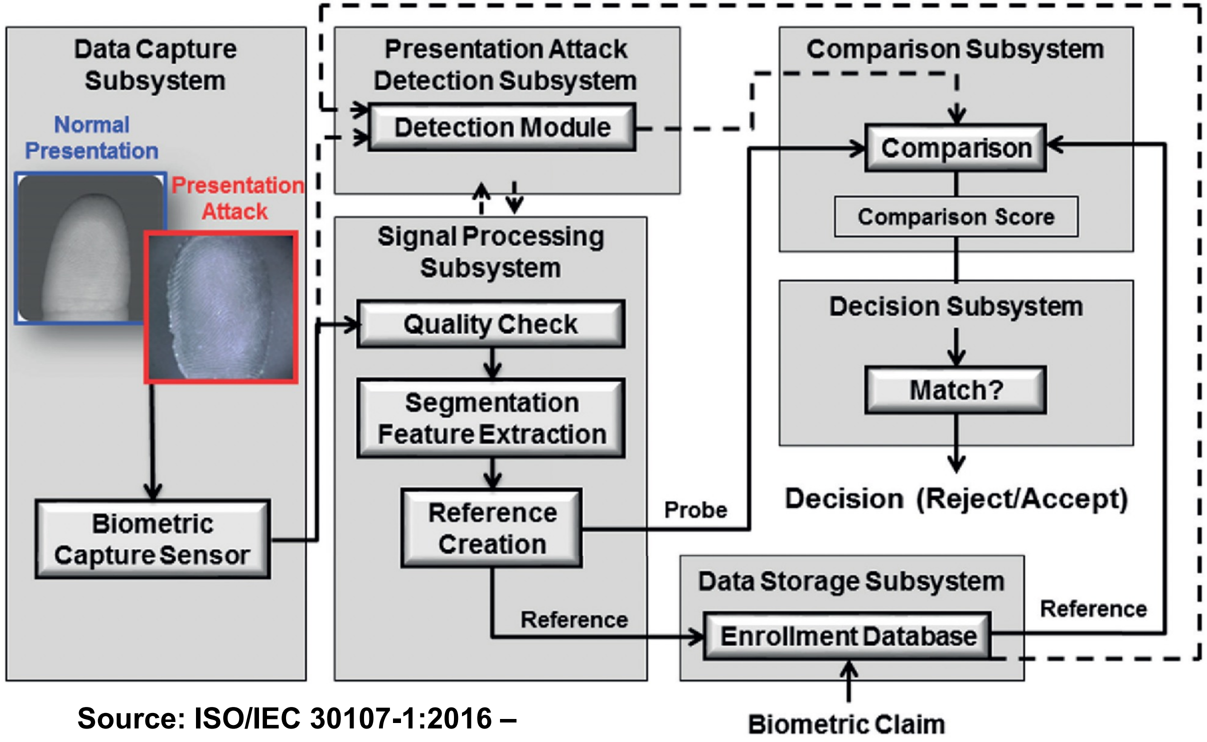
Accenture Federal Services

- Currently at DIS stage; a revision should be published in 2023
- **What's new -** draft aligns select terminology with *ISO/IEC 2382-37:2022* (*bona fide presentation, presentation attack, presentation attack detection, presentation attack instrument)*

Scope
This document establishes terms and definitions that are useful in the specification, characterization and evaluation of presentation attack detection methods.

Outside the scope are
— standardization of specific PAD detection methods;
— detailed information about countermeasures (i.e., anti-spoofing mechanisms), algorithms, or sensors;
— overall system-level security or vulnerability assessment.

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



Source: ISO/IEC 30107-1:2016 – Biometric presentation attack detection — Part 1: Framework

ISO/IEC 30107-2:2017 – Biometric presentation attack detection — Part 2: Data formats

- *ISO/IEC 30107-2:2017* is the only part of 30107 NOT under revision
- PAD data formats from *ISO/IEC 30107-2:2017* are now formally specified in ASN.1 and XML within *ISO/IEC 39794-1 – Extensible biometric data interchange formats — Part 1: Framework*

Scope (summarized)

This document defines data formats for conveying the mechanism used in biometric PAD and for conveying the results of PAD methods.

This document contains a binary format and an XML schema. The data interchange formats in this document are generic, in that they may be applied and used in a wide range of application areas. No application-specific requirements are addressed here.

Provisions for the cryptographic protection of the authenticity, integrity, and confidentiality of stored and transmitted presentation attack detection data are beyond the scope of this document

PAD output data elements

- PAD decision
- PAD mechanism vendor identifier
- PAD mechanism identifier
- PAD score
- PAD extended data mechanism vendor identifier
- PAD extended data mechanism identifier
- PAD extended data

PAD input data elements

- Context of capture
- Level of supervision / surveillance
- Risk level
- Category of criteria for PAD
- PAD parameters
- PAD challenges
- PAD data capture date and time
- Capture device vendor identifier
- Capture device model identifier
- Capture device serial number

ISO/IEC 30107-3:2017 – Biometric presentation attack detection — Part 3: Testing and Reporting

- Currently at FDIS stage; a revision should be published in 2023
- **What's new -** generalized metric, Relative Impostor Attack Presentation Accept Rate, reflecting tradeoffs between comparison (e.g., FRR) and PAD performance in full-system evaluations

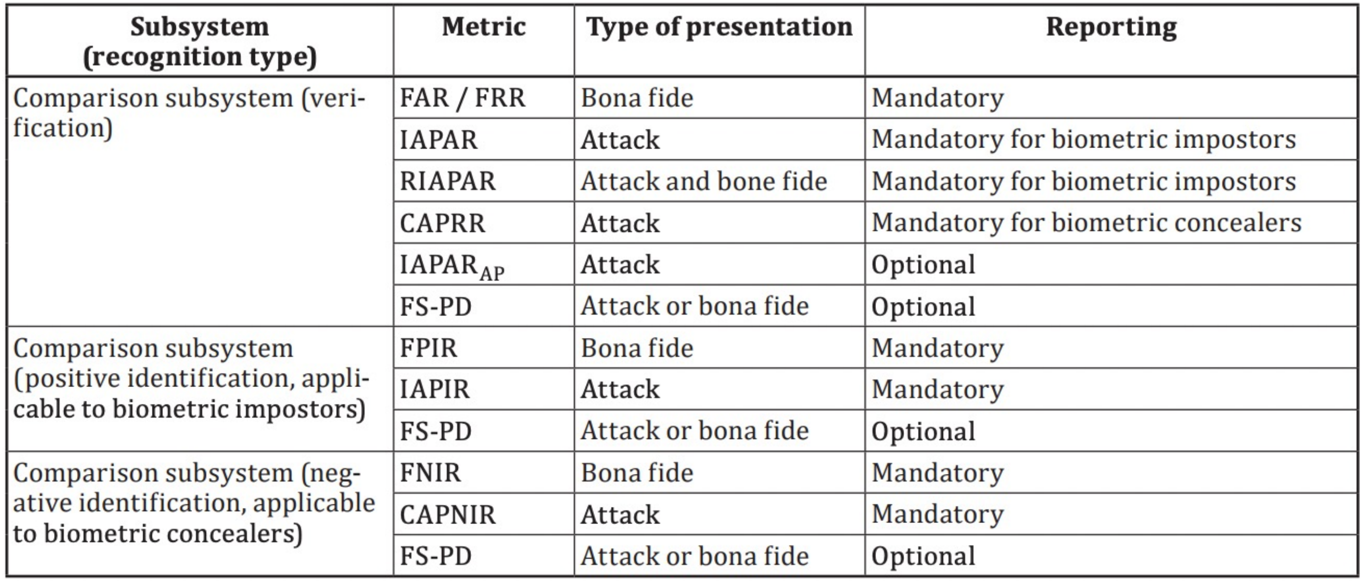
Scope (summarized)

This document establishes:

— principles and methods for performance assessment of PAD mechanisms;
— reporting of testing results from evaluations of PAD mechanisms;
— a classification of known attack types

Outside the scope are:

— standardization of specific PAD mechanisms;
— detailed information about countermeasures (anti-spoofing techniques), algorithms, or sensors;
— overall system-level security or vulnerability assessment



Subsystem (recognition type)	Metric	Type of presentation	Reporting
Comparison subsystem (verification)	FAR / FRR	Bona fide	Mandatory
	IAPAR	Attack	Mandatory for biometric impostors
	RIAPAR	Attack and bone fide	Mandatory for biometric impostors
	CAPRR	Attack	Mandatory for biometric concealers
	IAPAR_{AP}	Attack	Optional
	FS-PD	Attack or bona fide	Optional
Comparison subsystem (positive identification, applicable to biometric impostors)	FPIR	Bona fide	Mandatory
	IAPIR	Attack	Mandatory
	FS-PD	Attack or bona fide	Optional
Comparison subsystem (negative identification, applicable to biometric concealers)	FNIR	Bona fide	Mandatory
	CAPNIR	Attack	Mandatory
	FS-PD	Attack or bona fide	Optional

Source: FDIS ISO/IEC 30107-3 – Biometric presentation attack detection — Part 3: Testing and Reporting

ISO/IEC 30107-3:2017 – Biometric presentation attack detection — Part 4: Profile for Testing of Mobile Devices

- Currently at CD stage; a revision should be published in 2024
- **What's new -** an appendix with a profile directly aligned with **FIDO Biometrics Requirements** for biometric subsystems for use in mobile applications
- Examples of FIDO-specific parameters include the number of sources, species, and series used in a PAD evaluation

Scope (summarized)

This standard is a profile that specifies requirements for testing biometric 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 specific to mobile devices. It also establishes requirements 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.