INTERNATIONAL STANDARD

ISO/IEC 30107-2

First edition
2017-12

Information technology — Biometric presentation attack detection —

Part 2:
Data formats

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

Partie 2: Format des données

Reference number
ISO/IEC 30107-2:2017(E)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

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.

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 ISO documents 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 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).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on 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 the following URL: www.iso.org/iso/foreword.

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 30107 series can be found on the ISO website.

Introduction

The presentation of an artefact or of human characteristics to a biometric capture subsystem in a fashion that could interfere with the intended policy of the biometric system is referred to as a presentation attack. The ISO/IEC 30107 series is concerned with mechanisms for the automated detection of presentation attacks. These mechanisms are called presentation attack detection (PAD) mechanisms.

This document establishes common data formats for conveying the type of approach used in presentation attack detection and for conveying the results of presentation attack detection methods. This document specifies the meaning of the data elements used in the PAD data formats (see Clause 5), a tagged binary PAD data format based on an extensible specification in ASN.1 (see A.1), and a textual PAD data format based on an XML schema definition (see A.2). Annex A containing the formal specifications is normative. The informative Annex B gives encoding examples.

Information technology — Biometric presentation attack detection —

Part 2: Data formats

1 Scope

This document defines data formats for conveying the mechanism used in biometric presentation attack detection and for conveying the results of presentation attack detection methods. The attacks considered in the ISO/IEC 30107 series take place at the sensor during the presentation and collection of the biometric characteristics. Any other attacks are outside the scope of this document.

This document contains the following data formats: 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.

NOTE While addressing security is out of the scope of this document, PAD data may be protected by encoding them into a biometric information record (see ISO/IEC 19785-1) that includes an optional security block.

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 80000 (all parts), *Quantities and units*

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

ISO/IEC 8824-1, *Information technology — Abstract Syntax Notation One (ASN.1): Specification of basic notation*

ISO/IEC 8825-1, *Information technology — ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)*

ISO/IEC 19785-1, *Information technology — Common Biometric Exchange Formats Framework — Part 1: Data element specification*

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

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 2382-37 and ISO/IEC 30107-1 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 https://www.iso.org/obp

4 Conformance

A block of presentation attack detection (PAD) data shall be conformant to this document if it conforms to the normative requirements of Clause 5 and A.1 or A.2, respectively.

5 Data elements

5.1 Overview

Clause 5 contains a description of the data that may be generated by the PAD subsystem and used by a relying system. This data may be generated at any point in the system. Consequently, the PAD data available for a biometric sample may change at any stage in the collection and subsequent processing of the biometric sample. PAD subsystems have data inputs (such as thresholds, biometric samples, and secondary data streams, e.g. measures of conductance, reflectance, inductance, ECG, and challenge/response pairs) and provide output data.

Data relevant to PAD includes both input and output data streams. Output data may include:

a) an indication of whether PAD data is available (beyond that intrinsically embedded in the biometric signals);

b) an indication of whether a PAD decision has been made and, if so, the nature of the decision;

c) PAD score;

d) vector of partial PAD results;

e) any extended PAD data that accompanies the biometric sample;

f) identifiers of PAD mechanisms (PAD mechanism vendor identifier, PAD mechanism identifier, PAD extended data mechanism vendor identifier, and PAD extended data mechanism identifier).

Input data may include:

a) context of the capture — enrolment, verification, or identification;

b) level of supervision/surveillance during the capture process;

c) current risk level, e.g. recent attack activity;

d) category of criteria for PAD, i.e. the criteria are common for all subjects (global), are specific to each subject or are unknown;

e) any external parameters sent to be used in the PAD process;

f) any challenges that were given to the data capture subject;

g) PAD data capture date and time;

h) identifiers of the capture device (capture device vendor identifier, capture device model identifier, and capture device serial number).

NOTE Because there is a loose spatial and temporal binding between biometric samples and PAD data, the PAD output data need not be related only to a single acquired biometric sample. The PAD data may apply to other samples acquired during the transaction as well.

If physical and/or chemical magnitudes are included in the record, those magnitudes shall be expressed in units of the International System of Units (SI), as stated in ISO 80000 (all parts).

5.2 PAD output

5.2.1 PAD decision

Presence: Optional

Abstract values: ATTACK, NO_ATTACK, and FAILURE_TO_COMPUTE

NOTE The encoding of the abstract values in the tagged binary format is defined in A.1. The encoding of the abstract values in XML is defined in A.2.

Contents: If present, this data element shall indicate whether a presentation attack attempt has been detected by the PAD subsystem. The abstract value ATTACK shall indicate that a presentation attack attempt has been detected by the PAD subsystem. The abstract value NO_ATTACK shall indicate that no presentation attack attempt has been detected by the PAD subsystem. The abstract value FAILURE_TO_COMPUTE shall indicate that the PAD decision process has failed.

5.2.2 PAD mechanism vendor identifier

Presence: Optional

Abstract values: Integers 1 to 65 535

Contents: If present, this data element shall identify the vendor of the PAD mechanism. The vendor identifier shall be registered with the Biometric Registration Authority identified in ISO/IEC 19785-1.

5.2.3 PAD mechanism identifier

Presence: Conditional. This data element shall be included if and only if the PAD mechanism vendor identifier is present.

Abstract values: Integers 1 to 65 535

Contents: If present, this data element shall identify the PAD mechanism (referred to as PAD technique in ISO/IEC 19785-1). The PAD mechanism identifier shall be assigned by the PAD mechanism vendor.

Table 1 lists PAD mechanism identifiers for PAD approaches not connected with a particular vendor. For the PAD mechanism identifiers listed in Table 1, the biometric organization identifier of ISO/IEC JTC 1/SC 37, which is 257 (0101_{Hex}), shall be used as the PAD mechanism vendor identifier. These identifiers have been registered with the Biometric Registration Authority identified in ISO/IEC 19785-1.

Table 1 — PAD mechanism identifiers for PAD approaches not connected with a particular vendor

PAD mechanism vendor identifier	PAD mechanism identifier	Description
257 (0101_{Hex})	1 (0001_{Hex})	Challenge/involuntary response
257 (0101_{Hex})	2 (0002_{Hex})	Challenge/voluntary response
257 (0101_{Hex})	3 (0003_{Hex})	Challenge/response as a combination of what you are and know
257 (0101_{Hex})	4 (0004_{Hex})	Non-stimulated observation of liveness

5.2.4 PAD score

Presence: Optional

Abstract values: Integers 0 to 100 and FAILURE_TO_COMPUTE

Contents: If present, this data element shall indicate the PAD result as a score between 0 and 100. Bona-fide presentations shall tend to generate lower scores. Presentation attacks shall tend to generate higher scores. The abstract value FAILURE_TO_COMPUTE shall indicate that the computation of the PAD score has failed.

If the PAD score value is FAILURE_TO_COMPUTE, then, if present, the PAD decision value shall also be FAILURE_TO_COMPUTE.

5.2.5 PAD extended data mechanism vendor identifier

Presence: Conditional. This data element shall be included if and only if PAD extended data is present.

Abstract values: Integers 1 to 65 535

Contents: If present, this data element shall identify the vendor of the PAD mechanism used in the PAD extended data. The vendor identifier shall be registered with the Biometric Registration Authority identified in ISO/IEC 19785-1.

5.2.6 PAD extended data mechanism identifier

Presence: Conditional. This data element shall be included if and only if the PAD extended data vendor identifier is present.

Abstract values: Integers 1 to 65 535

Contents: If present, this data element shall identify the PAD mechanism used in the PAD extended data. The PAD extended data mechanism identifier shall be assigned by the PAD extended data mechanism vendor. The PAD mechanism identifier should be registered with the Biometric Registration Authority identified in ISO/IEC 19785-1.

NOTE ISO/IEC 19785-1:2015, 6.1.6 states that registration of biometric product identifiers is optional.

5.2.7 PAD extended data

Presence: Optional

Abstract values: Any octet string

Contents: If present, this data element shall include additional PAD-related information that cannot be held by the data elements defined above. The structure of this data is defined by the vendor of the identified mechanism.

5.3 PAD input

5.3.1 Context of capture

Presence: Optional

Abstract values: ENROLMENT, VERIFICATION, IDENTIFICATION

Contents: If present, this data element shall indicate the context of the capture process. The abstract value ENROLMENT shall indicate that the context of the capture process is enrolment. The abstract value VERIFICATION shall indicate that the context of the capture process is biometric verification. The abstract value IDENTIFICATION shall indicate that the context of the capture process is biometric identification.

5.3.2 Level of supervision/surveillance

Presence: Optional

Abstract values: UNKNOWN, CONTROLLED, ASSISTED, OBSERVED, UNATTENDED

Contents: If present, this data element shall indicate the level of supervision/surveillance during the capture process. Biometric authentication may be performed under a variety of conditions ranging from controlled to unattended, as shown in Table 2, which is based on Reference [4].

Table 2 — Device monitoring modes

Abstract value	Description
UNKNOWN	No information is known.
CONTROLLED	An operator physically controls the biometric capture subject to acquire biometric samples.
ASSISTED	A person is available to provide assistance to the biometric capture subject submitting the biometric characteristics.
OBSERVED	A person is present to observe operation of the device but provides no assistance[a].
UNATTENDED	No one is present to observe or provide assistance.

[a] This category includes observing user interaction with the biometric capture system through remote sensing, e.g. video surveillance, also known as telepresence.

5.3.3 Risk level

Presence: Optional

Abstract values: Integers 0 to 100

Contents: If present, this data element shall indicate the risk level as a score between 0 and 100, with lower scores being indicative of a lower risk and higher scores being indicative of a higher risk. If the risk level is unknown, then this data element shall not be present.

This field has been left vaguely defined so that system developers may devise their own qualitative or quantitative risk assessment methodologies.