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/IEC 2017



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2017, Published in Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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 ... **iv**
Introduction ... **v**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms and definitions ... **1**
4 Conformance ... **2**
5 Data elements ... **2**
5.1 Overview ... 2
5.2 PAD output ... 3
5.2.1 PAD decision ... 3
5.2.2 PAD mechanism vendor identifier ... 3
5.2.3 PAD mechanism identifier ... 3
5.2.4 PAD score ... 4
5.2.5 PAD extended data mechanism vendor identifier ... 4
5.2.6 PAD extended data mechanism identifier ... 4
5.2.7 PAD extended data ... 4
5.3 PAD input ... 5
5.3.1 Context of capture ... 5
5.3.2 Level of supervision/surveillance ... 5
5.3.3 Risk level ... 5
5.3.4 Category of criteria for PAD ... 6
5.3.5 PAD parameters ... 6
5.3.6 PAD challenges ... 6
5.3.7 PAD data capture date and time ... 6
5.3.8 Capture device vendor identifier ... 6
5.3.9 Capture device model identifier ... 7
5.3.10 Capture device serial number ... 7
Annex A (normative) **Formal specifications** ... **8**
Annex B (informative) **PAD encoding examples** ... **16**
Bibliography ... **17**

© ISO/IEC 2017 – All rights reserved

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.

© ISO/IEC 2017 – All rights reserved

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.

© ISO/IEC 2017 – All rights reserved

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

© ISO/IEC 2017 – All rights reserved