

AS ISO/IEC 30107.2:2024
ISO/IEC 30107-2:2017



STANDARDS
Australia



Information technology — Biometric presentation attack detection

Part 2: Data formats



AS ISO/IEC 30107.2:2024

This Australian Standard® was prepared by IT-032, Biometrics and Identification. It was approved on behalf of Standards Australia's Standards Development and Accreditation Committee on 04 August 2024.

This Standard was published on 6 September 2024.

The following are represented on Committee IT-032:

- Department of Defence (Australian Government)
- Department of Foreign Affairs and Trade (DFAT)
- Department of Home Affairs — Digital and Technology Policy Division
- Photo Marketing Association
- SITA

This Standard was issued in draft form for comment as DR AS ISO/IEC 30107.2:2024.

Keeping Standards up-to-date

Ensure you have the latest versions of our publications and keep up-to-date about Amendments, Rulings, Withdrawals, and new projects by visiting:

www.standards.org.au

ISBN 978 1 76139 817 9

Information technology — Biometric presentation attack detection

Part 2: Data formats

First published as AS ISO/IEC 30107.2:2024.

COPYRIGHT

© ISO/IEC 2024 — All rights reserved
© Standards Australia Limited 2024

All rights are reserved. No part of this work may be reproduced or copied in any form or by any means, electronic or mechanical, including photocopying, without the written permission of the publisher, unless otherwise permitted under the Copyright Act 1968 (Cth).

Preface

This Standard was prepared by the Standards Australia Committee IT-032, Biometrics and Identification.

The objective of this document is to define 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 AS 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 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 AS ISO/IEC 19785.1:2023) that includes an optional security block.

This document is identical with, and has been reproduced from, ISO/IEC 30107-2:2017, *Information technology — Biometric presentation attack detection — Part 2: Data formats*.

As this document has been reproduced from an international document, a full point substitutes for a comma when referring to a decimal marker.

Australian or Australian/New Zealand Standards that are identical adoptions of international normative references may be used interchangeably. Refer to the online catalogue for information on specific Standards.

The terms “normative” and “informative” are used in Standards to define the application of the appendices or annexes to which they apply. A “normative” appendix or annex is an integral part of a Standard, whereas an “informative” appendix or annex is only for information and guidance.

Contents

Preface	ii
Foreword	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Conformance	1
5 Data elements	2
5.1 Overview	2
5.2 PAD output	2
5.2.1 PAD decision	2
5.2.2 PAD mechanism vendor identifier	3
5.2.3 PAD mechanism identifier	3
5.2.4 PAD score	3
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	4
5.3.1 Context of capture	4
5.3.2 Level of supervision/surveillance	5
5.3.3 Risk level	5
5.3.4 Category of criteria for PAD	5
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	6
5.3.10 Capture device serial number	6
Annex A (normative) Formal specifications	7
Annex B (informative) PAD encoding examples	15
Bibliography	16

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.

NOTES