



**BSI Standards Publication**

**Document management — Portable  
Document Format — Integrity protection  
in encrypted documents in PDF 2.0**

---

## National foreword

This Published Document is the UK implementation of ISO/TS 32004:2024.

The UK participation in its preparation was entrusted to Technical Committee IDT/1, Document Management Applications.

A list of organizations represented on this committee can be obtained on request to its committee manager.

### Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

This publication is not to be regarded as a British Standard.

© The British Standards Institution 2024  
Published by BSI Standards Limited 2024

ISBN 978 0 539 17376 5

ICS 35.240.30; 37.100.99

### Compliance with a Published Document cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 31 May 2024.

### Amendments/corrigenda issued since publication

| Date | Text affected |
|------|---------------|
|------|---------------|



# Technical Specification

**ISO/TS 32004**

## **Document management — Portable Document Format — Integrity protection in encrypted documents in PDF 2.0**

*Gestion des documents — Format de document portable —  
Protection de l'intégrité dans les documents chiffrés en PDF 2.0*

**First edition  
2024-04**



**COPYRIGHT PROTECTED DOCUMENT**

© ISO 2024

All rights reserved. Unless otherwise specified, or required in the context of its implementation, 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  
CP 401 • Ch. de Blandonnet 8  
CH-1214 Vernier, Geneva  
Phone: +41 22 749 01 11  
Email: [copyright@iso.org](mailto:copyright@iso.org)  
Website: [www.iso.org](http://www.iso.org)

Published in Switzerland

# Contents

Page

|                                                                             |           |
|-----------------------------------------------------------------------------|-----------|
| <b>Foreword</b>                                                             | <b>iv</b> |
| <b>Introduction</b>                                                         | <b>v</b>  |
| <b>1 Scope</b>                                                              | <b>1</b>  |
| <b>2 Normative references</b>                                               | <b>1</b>  |
| <b>3 Terms and Definitions</b>                                              | <b>2</b>  |
| <b>4 Extension schema details</b>                                           | <b>3</b>  |
| <b>5 Proposed changes</b>                                                   | <b>3</b>  |
| 5.1 Encrypt dictionary                                                      | 3         |
| 5.1.1 Additions to ISO 32000-2:2020, 7.6.2                                  | 3         |
| 5.1.2 Additions to ISO 32000-2:2020, 7.6.4.2                                | 3         |
| 5.1.3 Additions to ISO 32000-2:2020, 7.6.5.2                                | 4         |
| 5.2 File trailer                                                            | 4         |
| 5.2.1 Additions to ISO 32000-2:2020, 7.5.5                                  | 4         |
| 5.2.2 Additions to ISO 32000-2:2020, 7.6.2                                  | 4         |
| 5.2.3 AuthCode dictionary                                                   | 4         |
| <b>6 Composing PDF MAC tokens</b>                                           | <b>6</b>  |
| 6.1 General                                                                 | 6         |
| 6.2 <i>PdfMacIntegrityInfo</i> data type                                    | 6         |
| 6.3 CMS structure of a PDF MAC token                                        | 6         |
| 6.3.1 General                                                               | 6         |
| 6.3.2 Encapsulated content info of a PDF MAC token                          | 6         |
| 6.3.3 Recipient info object, MAC key generation and key encryption          | 6         |
| 6.3.4 Digest algorithm identification                                       | 7         |
| 6.3.5 MAC algorithm identification                                          | 7         |
| 6.3.6 Authenticated attributes                                              | 7         |
| 6.3.7 Unauthenticated attributes                                            | 8         |
| 6.4 Key derivation function                                                 | 8         |
| 6.5 Location of PDF MAC tokens                                              | 9         |
| 6.5.1 Location of a PDF MAC token in an unsigned revision                   | 9         |
| 6.5.2 Location of a PDF MAC token in a signed revision                      | 9         |
| 6.6 Computing the digests in a PDF MAC token                                | 9         |
| 6.6.1 General                                                               | 9         |
| 6.6.2 PDF MAC digests in unsigned revisions                                 | 10        |
| 6.6.3 PDF MAC digests in signed revisions                                   | 10        |
| <b>Annex A (informative) ASN.1 module for PDF MAC</b>                       | <b>11</b> |
| <b>Annex B (informative) Validation of document integrity using PDF MAC</b> | <b>12</b> |
| <b>Annex C (informative) Examples</b>                                       | <b>14</b> |
| <b>Bibliography</b>                                                         | <b>16</b> |

## Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

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 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](http://www.iso.org/directives)).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes 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 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](http://www.iso.org/patents). ISO 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](http://www.iso.org/iso/foreword.html).

This document was prepared by Technical Committee ISO/TC 171, *Document management applications*, Subcommittee SC 2, *Document file formats, EDMS systems and authenticity of information*.

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](http://www.iso.org/members.html).

## Introduction

When encrypting documents, it is important to not only preserve the confidentiality of the encrypted material, but also to ensure that the receiving party can verify its integrity. Encryption mechanisms defined in ISO 32000-2:2020 currently only provide confidentiality without this authentication aspect.

This document describes a mechanism to protect the integrity of an encrypted PDF document using a Message Authentication Code (MAC), with key material derived from the file encryption key. Message authentication codes are distinct from digital signatures based on public-key cryptography. Digital signatures and message authentication codes have different but complementary security properties: a valid MAC created following this document proves knowledge of the file encryption key, whereas digital signatures as defined in ISO 32000-2:2020 do not have that property.

The MAC mechanism described in this document is backwards compatible with ISO 32000-2:2020 and can also be used in PDF documents containing digital signatures.

This document follows the lexical conventions regarding the usage of bold and italics which are specified in ISO 32000-2:2020, Clause 4.

