ISO/~~TS~~ DTS 32004:~~202x(X~~2024(E)

ISO/TC 171/SC 2~~/WG 8~~

Secretariat: ANSI

Date: ~~2023-10-23~~2024-01-19

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

~~DTS stage~~

~~Warning for WDs and CDs~~

~~This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.~~

~~Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.~~

Style Definition ...
Formatted: Font: 11 pt, French (Switzerland)
Formatted ...
Formatted: zzCover, Left
Formatted ...
Formatted: French (Switzerland)
Formatted: French (Switzerland)
Formatted: zzCover, Left, Space After: 0 pt
Formatted: Font: 11 pt, French (Switzerland)
Formatted: zzCover, Line spacing: single, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted: Font: 11 pt, French (Switzerland)

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

ISO copyright office

CP 401 • Ch. de Blandonnet 8

CH-1214 Vernier, Geneva

Phone: +41 22 749 01 11

Email: copyright@iso.org

Website: ~~www.iso.org~~www.iso.org

Published in Switzerland

Formatted: Indent: Left: 0 cm, Right: 0 cm

Formatted: Indent: Left: 0 cm, First line: 0 cm, Right: 0 cm

Formatted: Indent: Left: 0 cm, Right: 0 cm

Contents Page

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 ~~documents~~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~~www.iso.org/directives).

~~Attention is drawn~~ISO draws attention to the possibility that ~~some of~~ the ~~elements~~implementation of this document may ~~be~~involve the ~~subject~~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. 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 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~~ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see ~~www.iso.org/iso/foreword.html~~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~~www.iso.org/members.html.

Formatted: Foreword Text
Formatted: English (United States)
Formatted: Font: Italic
Formatted: Foreword Text, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted: Font: Italic
Formatted: English (United States)
Formatted: Foreword Text
Formatted: English (United States)

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.

Formatted: std_publisher
Formatted: std_docNumber
Formatted: std_docPartNumber
Formatted: std_year
Formatted: Font: Not Bold
Formatted: std_publisher
Formatted: std_docNumber
Formatted: std_docPartNumber
Formatted: std_year
Formatted: std_publisher
Formatted: std_docNumber
Formatted: std_docPartNumber
Formatted: std_year

Formatted: Space After: 0 pt, Line spacing: single

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

Formatted: Font: 11 pt

Formatted: Space After: 0 pt, Line spacing: single

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

1 Scope

This document specifies how to extend the ISO 32000-2:2020 specification by adding extensions to the **Encrypt** dictionary and trailer dictionary to provide integrity protection to the encrypted PDF document. This document also ensures that extensions are fully backward-compatible.

These extensions are intended for developers of software that creates PDF files (PDF writers), software that reads existing PDF files and (usually) interprets their contents for display (PDF readers), software that reads and displays PDF content and interacts with the computer users to possibly modify and save the PDF file (interactive PDF processors) and PDF products that read and/or write PDF files for a variety of other purposes (PDF processors).

NOTE PDF writers and PDF readers are more specialized classifications of interactive PDF processors and ~~all~~both are PDF processors.

This document does not specify the following:

- — specific processes for converting paper or electronic documents to the PDF file format;
- — specific technical design, user interface implementation, or operational details of rendering;
- — specific physical methods of storing these documents such as media and storage conditions;
- — methods for validating the conformance of PDF files or PDF processors;
- — required computer hardware and/or operating system.

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- 32000-2:2020, *Document management — Portable ~~Document Format~~document format — Part 2: PDF- 2.0*

~~IETF RFC 5652: *Cryptographic Message Syntax (CMS).* [online]. 2009. Available from: https://tools.ietf.org/html/rfc5652.html~~

~~IETF RFC 3394: *Advanced Encryption Standard (AES) Key Wrap Algorithm.* [online]. 2002. Available from: https://tools.ietf.org/html/rfc3394.html~~

~~NIST Computer Security Objects Register (CSOR). [online]. 2009. Available from: https://csrc.nist.gov/projects/computer-security-objects-register~~

Formatted: Section start: New page, Different first page header
Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted: std_publisher
Formatted: std_docNumber
Formatted: std_docPartNumber
Formatted: std_year
Formatted: Note, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers, Tab stops: 0.7 cm, Left + 1.4 cm, Left + 2.1 cm, Left + 2.8 cm, Left + 3.5 cm, Left + 4.2 cm, Left + 4.9 cm, Left + 5.6 cm, Left + 6.3 cm, Left + 7 cm, Left
Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted: List Continue 1, No bullets or numbering, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers, Tab stops: 0.7 cm, Left + 1.4 cm, Left + 2.1 cm, Left + 2.8 cm, Left + 3.5 cm, Left + 4.2 cm, Left + 4.9 cm, Left + 5.6 cm, Left + 6.3 cm, Left + 7 cm, Left
Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted: Body Text
Formatted: std_publisher
Formatted: RefNorm, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers, Tab stops: 0.7 cm, Left + 1.4 cm, Left + 2.1 cm, Left + 2.8 cm, Left + 3.5 cm, Left + 4.2 cm, Left + 4.9 cm, Left + 5.6 cm, Left + 6.3 cm, Left + 7 cm, Left
Formatted: std_docNumber
Formatted: std_docPartNumber
Formatted: std_year
Formatted: std_docTitle, Font: Not Italic
Formatted: std_docTitle, Font: Not Italic
Formatted: std_docTitle, Font: Not Italic
Formatted: Font: Not Italic
Formatted: std_docTitle
Formatted: bib_year