Technical Specification

ISO/TS 32001:2022

These PDF Association members have made this copy of ISO/TS 32001:2022 available to you:

Visit
https://pdfa.org/sponsored-standards/
for the latest information & updates

PDF Association, Inc. 10 Longfellow Road, Winchester, MA 01890, USA
PDF Association e.V., Friedenstr. 2A, 16321 Bernau bei Berlin, Germany
pdfa.org

TECHNICAL SPECIFICATION

ISO/TS 32001

First edition
2022-09

Document management — Portable Document Format — Extensions to Hash Algorithm Support in ISO 32000-2 (PDF 2.0)

Gestion de documents — Format de document portable (PDF) — Extensions pour la prise en charge de l'algorithme de hachage dans l'ISO 32000-2 (PDF 2.0)

Reference number
ISO/TS 32001:2022(E)

COPYRIGHT PROTECTED DOCUMENT

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

Published in Switzerland

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 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 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.

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.

Introduction

Hash algorithms and encryption are a fundamental part of the ISO 32000 series. ISO 32000-2 updated both hash algorithms and encryption, but in the time since that standard was published, new algorithms have been developed or risen to prominence.

To ensure that PDF remains relevant in the fast-moving world of cryptography and remains current with best practices, these techniques should be refreshed and updated regularly. This document builds upon the mechanisms present in ISO 32000-2 and extends and enhances them to meet the latest needs of the industry.

Document management — Portable Document Format — Extensions to Hash Algorithm Support in ISO 32000-2 (PDF 2.0)

1 Scope

This document specifies how to extend the specifications in ISO 32000-2 by adding support for the use of the Secure Hash Algorithm – 3 (SHA-3) and SHAKE256 hash algorithms.

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.

IETF RFC 8419, Use of Edwards-Curve Digital Signature Algorithm (EdDSA) Signatures in the Cryptographic Message Syntax (CMS).[1)]

ISO 32000-2, *Document management — Portable document format — Part 2: PDF 2.0*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
portable document format
PDF
file format defined in ISO 32000-2

4 Extension schema details

PDF documents using enhancements described in this document shall include in their document catalogue dictionary (see ISO 32000-2:2020, 7.7.2) an extensions dictionary (see ISO 32000-2:2020,7.12)

1) Available at: https://datatracker.ietf.org/doc/html/rfc8419

with a prefix name of **ISO_**. This shall contain a developer extensions dictionary in accordance with ISO 32000-2:2020, 7.12.3, with the following entries as shown in Table 1.

Table 1 — Developer extensions dictionary values for documents using enhancements described in this document

Key	Type	Value
BaseVersion	name	2.0
ExtensionLevel	integer	32001
ExtensionRevision	text string	:2022
Type	name	DeveloperExtensions
URL	string	https://www.iso.org/standard/45874.html

5 Digital signature enhancements

5.1 Support for secure hash algorithm 3 (SHA-3) hash family

5.1.1 General

PDF 2.0 supports a variety of hash algorithms for generating digests for the purposes of digitally signing PDF documents. This document adds support for digitally signing PDF documents using the SHA3-256, SHA3-384, SHA3-512 and SHAKE256 hash algorithms in the secure hash algorithm 3 (SHA-3) hash algorithm family as defined in FIPS PUB 202.

5.1.2 Addition to ISO 32000-2:2020, Table 237 — Entries in a signature field seed value dictionary

In ISO 32000-2:2020, Table 237 (“Entries in a signature field seed value dictionary”; section 12.7.5.5, “Signature fields”), the following text is added to the end of the current **DigestMethod** value text:

(PDF 2.x) In addition to those values previously defined, this value may be one of SHA3-256, SHA3-384, SHA3-512 or SHAKE256.

5.1.3 Changes to ISO 32000-2:2020, Table 256 — Entries in a signature reference dictionary

In ISO 32000-2:2020, Table 256 (“Entries in a signature reference dictionary”; 12.8.1, “General”), the following text is added to the end of the current **DigestMethod** value text:

(PDF 2.x) In addition to those values previously defined, this value may be one of SHA3-256, SHA3-384, SHA3-512 or SHAKE256. Default value for PDF 2.0: SHA256 (PDF 2.0).

5.1.4 Changes to ISO 32000-2:2020, Table 260 — SubFilter value algorithm support

In ISO 32000-2:2020, Table 260 (“SubFilter value algorithm support”; 12.8.3.1, “General”), the following values are added to the Message Digest value entry for **adbe.pkcs7.detached, ETSI.CAdES.detached or ETSI.RFC3161**:

— SHA3-256 (PDF 2.x)

— SHA3-384 (PDF 2.x)

— SHA3-512 (PDF 2.x)

— SHAKE256 (PDF 2.x). When SHAKE256 is specified, the message digest algorithm identified by the id-shake256 object identifier (OID) in section 2.3 of RFC 8419 shall be used.

NOTE The requirement to use the id-shake256 OID fixes the SHAKE256 output length for the digest at 512 bits and serves to prohibit variable length SHAKE256 algorithm usage and prohibit use of SHAKE256 algorithms with OIDs other than id-shake256.

Bibliography

[1] FIPS PUB 202, *SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions, NIST, August 2015*.[2)]

2) https://csrc.nist.gov/publications/detail/fips/202/final

ICS 35.240.30; 37.100.99

Price based on 4 pages