Technical Specification

ISO/TS 32002:2022

These PDF Association members have made this copy of ISO/TS 32002:2022 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 32002

First edition
2022-10

Document management — Portable Document Format — Extensions to Digital Signatures in ISO 32000-2 (PDF 2.0)

Gestion de documents — Format de document portable — Extensions pour les signatures numériques dans l'ISO 32000-2 (PDF 2.0)

Reference number
ISO/TS 32002:2022(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 ..... **iv**
Introduction ..... **v**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **1**
4 Extension Schema Details **2**
5 Digital signature enhancements **2**
5.1 Elliptic curve cryptography 2
5.1.1 Specification of allowed elliptic curve algorithms 2
5.1.2 Proposed changes to ISO 32000-2:2020 Table 260 – SubFilter value algorithm support 2
5.1.3 Specification of allowed elliptic curves 3
5.1.4 Hash algorithm congruence for message digest and signed attribute digest 3
Bibliography **4**

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

Digital signatures are a fundamental part of the ISO 32000 series. ISO 32000-2 contains updated digital signature support, 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 Digital Signatures in ISO 32000-2 (PDF 2.0)

1 Scope

This document specifies how to extend the ISO 32000-2 specification by adding support for the following:

— use of the NIST P-curve family of elliptical curves for digital signatures;

— use of the Brainpool family of elliptical curves for digital signatures;

— use of Edwards Curve (EdDSA) Ed448 and Ed25519 families of elliptical curves for digital signatures.

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 — Part 2: PDF 2.0*

ISO/TS 32001, *Document management — Portable Document Format — Extensions to Hash Algorithm Support in ISO 32000-2 (PDF 2.0)*

IETF RFC 5480:2009, *Elliptic Curve Cryptography Subject Public Key Information*[1)]

IETF RFC 5753:2010, *Use of Elliptic Curve Cryptography (ECC) Algorithms in Cryptographic Message Syntax (CMS)*[2)]

IETF RFC 8419:2018, *Use of Edwards-Curve Digital Signature Algorithm (EdDSA) Signatures in the Cryptographic Message Syntax (CMS)*[3)]

3 Terms and definitions

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

1) https://datatracker.ietf.org/doc/html/rfc5480

2) https://datatracker.ietf.org/doc/html/rfc5753

3) https://datatracker.ietf.org/doc/html/rfc8419

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
PDF (Portable Document Format)
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) 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	32002
ExtensionRevision	text string	:2022
Type	name	DeveloperExtensions
URL	string	https://www.iso.org/standard/45875.html

5 Digital signature enhancements

5.1 Elliptic curve cryptography

5.1.1 Specification of allowed elliptic curve algorithms

PDF 2.0 supports elliptic curve cryptography for digital signatures using the Elliptic Curve Digital Signature Algorithm (ECDSA) as defined in ANSI X9.62 and specified in ISO 32000-2:2020, Table 260. This document extends the elliptic curve digital signature support in Table 260 to add support for more recent ECDSA curves, as defined in IETF RFCs 5639 and 6932, and to add support for Edwards-curve Digital Signature Algorithm (EdDSA) based digital signatures as defined in IETF RFC 8419.

5.1.2 Proposed changes to ISO 32000-2:2020 Table 260 – SubFilter value algorithm support

In order to add support for EdDSA-based digital signatures, the following row and footnote are added to ISO 32000-2:2020, Table 260, as shown in Table 2.

Table 2 — Additional permitted SubFilter values for ISO 32000-2:2020, Table 260

SubFilter value	adbe.pkcs7.detached, ETSI.CAdES.detached or ETSI.RFC3161	adbe.pkcs7.sha1 (c)	adbe.x509.rsa_sha1 (a)
EdDSA algorithm support	IETF RFC 8032, Edwards-curve Digital Signature Algorithm (EdDSA) (PDF 2.x) using the Ed25519 or Ed448 elliptic curves[b]	No	No

[b] When using the Ed25519 EdDSA elliptic curve algorithm, the message digest shall be computed using the SHA512 message digest algorithm with OID id-sha512 as defined in IETF RFC 8419:2018, 2.3. When using the Ed448 EdDSA elliptic curve algorithm, the message digest shall be computed using the SHAKE256 message digest algorithm with OID id-shake256 as defined in IETF RFC 8419:2018, 2.3.

5.1.3 Specification of allowed elliptic curves

The text in Table 3 is appended to the end of ISO 32000-2:2020, 12.8.3.1 to enumerate recognized values for ECDSA and EdDSA elliptic curves and the SHA and SHA-3 digest algorithms (as defined in FIPS PUB 202) that are supported for these ECDSA and EdDSA elliptic curves.

Table 3 defines ECDSA elliptic curves and associated message digest algorithms supported for the adbe.pkcs7.detached, ETSI.CAdES.detached or ETSI.RFC3161 SubFilter values in ISO 32000-2:2020, Table 260.

Table 3 — Supported ECDSA elliptic curves

Elliptic curve name	Digest algorithms
P-256	SHA-256, SHA3–256
P-384	SHA-384, SHA3–384
P-521	SHA512, SHA3–512
brainpoolP256r1	SHA256, SHA384, SHA512, SHA3–256, SHA3–384, SHA3–512
brainpoolP384r1	SHA384, SHA512, SHA3–384, SHA3–512
brainpoolP512r1	SHA512, SHA3–512

NOTE 1 BSI Technical Guideline TR-03111 provides usage guidance for the brainpool family of elliptic curves.

When using the ECDSA elliptic curves in Table 1 for signing data, these shall be used in accordance with the requirements and recommendations in IETF RFC 5480 and IETF RFC 5753. Certificates for ECDSA keys used in PDF signatures shall specify curve parameters (ECParameters) for the subject's public key using the namedCurve option, in accordance with IETF RFC 5480:2009, section 2.1.1. The implicitCurve and specifiedCurve options shall not be used.

NOTE 2 This restriction implies that ECDSA signature values are required to be represented using the DER-encoded ECDSA-Sig-Value type in IETF RFC 5753:2010, section 7.2.

Table 4 defines EdDSA elliptic curves and associated message digest algorithms supported for the adbe.pkcs7.detached, ETSI.CAdES.detached or ETSI.RFC3161 SubFilter values in ISO 32000-2:2020, Table 260.

Table 4 — Supported EdDSA elliptic curves

Elliptic curve name	Digest algorithms	Restrictions
Ed25519	SHA512	
Ed448	SHAKE256	Message digests shall be calculated using the fixed length id-shake256 message digest algorithm in accordance with ISO/TS 32001.

PDF processors may ignore or handle in an implementation-dependent manner PDF documents which are signed with elliptic curves not listed in Table 3 or Table 4.

NOTE 3 The use of unnamed curves that do not have a published object ID contradicts security best practices.

5.1.4 Hash algorithm congruence for message digest and signed attribute digest

In order to more precisely specify how message digest algorithms shall be used with elliptic curves, the following text is added after ISO 32000-2: 2020, 5.1.2.

If the signedAttrs field is present in the SignerInfo field for the signer, then the same message digest algorithm shall be used to compute both the digest of the SignedData encapContentInfo eContent and the digest of the DER-encoded signedAttrs passed to the signature algorithm.

Bibliography

[1] BSI Technical Guideline TR-03111, Elliptic Curve Cryptography Version 2.10.[4)]

[2] The Elliptic Curve Digital Signature Algorithm (ECDSA), ANSI X9.62-2005, American National Standard for Financial Services, November 16, 2005.

[3] FIPS PUB 202, *SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions. NIST, August 2015*.[5)]

[4] IETF RFC 5639, *Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation*.[6)]

[5] IETF RFC 5652, *Cryptographic Message Syntax*.[7)]

[6] IETF RFC 6932, *Brainpool Elliptic Curves for the Internet Key Exchange (IKE) Group Description Registry*.[8)]

[7] IETF RFC 8032, *Edwards-Curve Digital Signature Algorithm (EdDSA)*.[9)]

[8] IETF RFC 8933, *Update to the Cryptographic Message Syntax (CMS) for Algorithm Identifier Protection*.[10)]

4) https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03111/BSI-TR-03111_V-2-1_pdf.pdf?__blob=publicationFile&v=1

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

6) https://datatracker.ietf.org/doc/html/rfc5639/

7) https://datatracker.ietf.org/doc/html/rfc5652

8) https://datatracker.ietf.org/doc/html/rfc6932/

9) https://datatracker.ietf.org/doc/html/rfc8032/

10) https://datatracker.ietf.org/doc/html/rfc8933

ICS 35.240.30; 37.100.99

Price based on 4 pages