ISO DTS /TS 32002:202#(X2022(E)

Date: 2022-08-08

ISO TC 171 / SC 2 / WG 8

Secretariat: ANSI

Document management — Portable Document Format — Extensions to Digital Signatures in ISO 32000-2 (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.

ISO copyright office
Copyright Office

CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva

Phone: +41 22 749 01 11
Fax: +41 22 749 09 47

Email: copyright@iso.org
copyright@iso.org

Website: www.iso.orgwww.iso.org

Published in Switzerland.

Contents

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 ~~need to~~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 use of the NIST P-curve family of elliptical curves for digital signatures;

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

— Use 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 — ~~Part 2: PDF 2.0~~Extensions to Hash Algorithm Support in ISO 32000-2 (PDF 2.0)*

IETF RFC 5480:2009, *Elliptic Curve Cryptography Subject Public Key Information ~~https://datatracker.ietf.org/doc/html/rfc5480~~*[1]

IETF RFC 5753:2010, *Use of Elliptic Curve Cryptography (ECC) Algorithms in Cryptographic Message Syntax (CMS~~). https://datatracker.ietf.org/doc/html/rfc5753~~*)[2]

[1] https://datatracker.ietf.org/doc/html/rfc5480
[2] https://datatracker.ietf.org/doc/html/rfc5753

IETF RFC 8419:2018, *Use of Edwards-Curve Digital Signature Algorithm (EdDSA) Signatures in the Cryptographic Message Syntax (CMS)*. https://datatracker.ietf.org/doc/html/rfc8419

2
© ISO 2022 – All rights reserved