This is a preview of "DS/ISO/TS 32002:2022". Click here to purchase the full version from the ANSI store.

Dokumentstyring – Portable document format – Udvidelser til digitale signaturer i ISO 32000-2 (PDF 2.0)

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

DANSK STANDARD
Danish Standards Association

Göteborg Plads 1
DK-2150 Nordhavn

Tel: +45 39 96 61 01
dansk.standard@ds.dk
www.ds.dk

© Dansk Standard - Eftertryk uden tilladelse forbudt

This is a preview of "DS/ISO/TS 32002:2022". Click here to purchase the full version from the ANSI store.

DS projekt: M362873
ICS: 35.240.30; 37.100.99

Første del af denne publikations betegnelse er:
DS/ISO/TS, hvilket betyder, at det er en international teknisk specifikation, der har status som DS-information.

Denne publikations overensstemmelse er:
IDT med: ISO/TS 32002:2022

DS-publikationen er på engelsk.

DS-publikationstyper
Dansk Standard udgiver forskellige publikationstyper.
Typen på denne publikation fremgår af forsiden.

Der kan være tale om:

Dansk standard
- standard, der er udarbejdet på nationalt niveau, eller som er baseret på et andet lands nationale standard, eller
- standard, der er udarbejdet på internationalt og/eller europæisk niveau, og som har fået status som dansk standard

DS-information
- publikation, der er udarbejdet på nationalt niveau, og som ikke har opnået status som standard, eller
- publikation, der er udarbejdet på internationalt og/eller europæisk niveau, og som ikke har fået status som standard, fx en teknisk rapport, eller
- europæisk præstandard

DS-håndbog
- samling af standarder, eventuelt suppleret med informativt materiale

DS-hæfte
- publikation med informativt materiale

Til disse publikationstyper kan endvidere udgives
- tillæg og rettelsesblade

DS-publikationsform
Publikationstyperne udgives i forskellig form som henholdsvis
- fuldtekstpublikation (publikationen er trykt i sin helhed)
- godkendelsesblad (publikationen leveres i kopi med et trykt DS-omslag)
- elektronisk (publikationen leveres på et elektronisk medie)

DS-betegnelse
Alle DS-publikationers betegnelse begynder med DS efterfulgt af et eller flere præfikser og et nr., fx **DS 383**, **DS/EN 5414** osv. Hvis der efter nr. er angivet et **A** eller **Cor**, betyder det, enten at det er et **tillæg** eller et **rettelsesblad** til hovedstandarden, eller at det er indført i hovedstandarden.
DS-betegnelse angives på forsiden.

Overensstemmelse med anden publikation:
Overensstemmelse kan enten være IDT, EQV, NEQ eller MOD
- **IDT:** Når publikationen er identisk med en given publikation.
- **EQV:** Når publikationen teknisk er i overensstemmelse med en given publikation, men præsentationen er ændret.
- **NEQ:** Når publikationen teknisk eller præsentationsmæssigt ikke er i overensstemmelse med en given standard, men udarbejdet på baggrund af denne.
- **MOD:** Når publikationen er modificeret i forhold til en given publikation.

TECHNICAL ISO/TS

This is a preview of "DS/ISO/TS 32002:2022". Click here to purchase the full version from the ANSI store.

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)

© ISO 2022

This is a preview of "DS/ISO/TS 32002:2022". Click here to purchase the full version from the ANSI store.

COPYRIGHT PROTECTED DOCUMENT

© ISO 2022, Published in Switzerland

All rights reserved. Unless otherwise specified, 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
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

© ISO 2022 – All rights reserved

This is a preview of "DS/ISO/TS 32002:2022". Click here to purchase the full version from the ANSI store.

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**

© ISO 2022 – All rights reserved

This is a preview of "DS/ISO/TS 32002:2022". Click here to purchase the full version from the ANSI store.

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.

© ISO 2022 – All rights reserved

This is a preview of "DS/ISO/TS 32002:2022". Click here to purchase the full version from the ANSI store.

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.

© ISO 2022 – All rights reserved

This is a preview of "DS/ISO/TS 32002:2022". Click here to purchase the full version from the ANSI store.

This is a preview of "DS/ISO/TS 32002:2022". Click here to purchase the full version from the ANSI store.

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)]

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 2022 – All rights reserved