

# ISO/TS 32004:2024-04 (E)

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

---

### Contents

Page

- Foreword ..... iv
- Introduction ..... v
- 1 Scope ..... 1
- 2 Normative references ..... 1
- 3 Terms and Definitions ..... 2
- 4 Extension schema details ..... 3
- 5 Proposed changes ..... 3
  - 5.1 Encrypt dictionary ..... 3
    - 5.1.1 Additions to ISO 32000-2:2020, 7.6.2 ..... 3
    - 5.1.2 Additions to ISO 32000-2:2020, 7.6.4.2 ..... 3
    - 5.1.3 Additions to ISO 32000-2:2020, 7.6.5.2 ..... 4
  - 5.2 File trailer ..... 4
    - 5.2.1 Additions to ISO 32000-2:2020, 7.5.5 ..... 4
    - 5.2.2 Additions to ISO 32000-2:2020, 7.6.2 ..... 4
    - 5.2.3 AuthCode dictionary ..... 4
- 6 Composing PDF MAC tokens ..... 6
  - 6.1 General ..... 6
  - 6.2 PdfMacIntegrityInfo data type ..... 6
  - 6.3 CMS structure of a PDF MAC token ..... 6
    - 6.3.1 General ..... 6
    - 6.3.2 Encapsulated content info of a PDF MAC token ..... 6
    - 6.3.3 Recipient info object, MAC key generation and key encryption ..... 6
    - 6.3.4 Digest algorithm identification ..... 7
    - 6.3.5 MAC algorithm identification ..... 7
    - 6.3.6 Authenticated attributes ..... 7
    - 6.3.7 Unauthenticated attributes ..... 8
  - 6.4 Key derivation function ..... 8
  - 6.5 Location of PDF MAC tokens ..... 9
    - 6.5.1 Location of a PDF MAC token in an unsigned revision ..... 9
    - 6.5.2 Location of a PDF MAC token in a signed revision ..... 9
  - 6.6 Computing the digests in a PDF MAC token ..... 9
    - 6.6.1 General ..... 9
    - 6.6.2 PDF MAC digests in unsigned revisions ..... 10
    - 6.6.3 PDF MAC digests in signed revisions ..... 10
- Annex A (informative) ASN.1 module for PDF MAC ..... 11
- Annex B (informative) Validation of document integrity using PDF MAC ..... 12
- Annex C (informative) Examples ..... 14
- Bibliography ..... 16