International Standard

ISO 14533-3

Second edition
2025-10

Processes, data elements and documents in commerce, industry and administration — Long-term signature —

Part 3: Profiles for PDF Advanced Electronic Signatures (PAdES)

Processus, éléments d'informations et documents dans le commerce, l'industrie et l'administration — Signature à long terme —

Partie 3: Profils pour les signatures électroniques avancées des PDF (PAdES)

Reference number
ISO 14533-3:2025(en)

© ISO 2025



COPYRIGHT PROTECTED DOCUMENT

© ISO 2025
All rights reserved. Unless otherwise specified, or required in the context of its implementation, 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
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 Abbreviated terms ... **2**
5 Requirements ... **3**
5.1 Conformity to PAdES-T ... 3
5.2 Conformity to PAdES-A ... 3
5.3 Conformity to PAdES-DT/DTA ... 3
5.4 Declaration of conformity ... 3
6 Long-term signature profiles ... **3**
6.1 Definition of PAdES profile and positioning ... 3
6.2 Representation of the required level ... 4
6.3 Standard for setting the required level ... 4
6.4 PAdES-T profile ... 5
6.4.1 General ... 5
6.4.2 PAdES using CAdES signatures profile ... 6
6.4.3 Timestamp of PAdES-T profile ... 9
6.5 PAdES-A profile ... 9
6.5.1 General ... 9
6.5.2 Structure of the PAdES-A profile ... 9
6.5.3 Document security store dictionary ... 10
6.5.4 Signature VRI dictionary ... 10
6.5.5 Document timestamp ... 10
6.5.6 Updating PAdES-A ... 11
6.5.7 Validation data for signature and timestamp ... 11
6.6 Multiple signatures ... 11
6.6.1 General ... 11
6.6.2 Timestamp for multiple signatures ... 12
Annex A (informative) **Supplier's declaration of conformity and its attachment** ... **13**
Annex B (normative) **The profile for using only timestamp** ... **18**
Annex C (normative) **Structure of timestamp token** ... **20**
Annex D (informative) **Applying PAdES using CMS signatures** ... **22**
Annex E (informative) **Examples of multiple signatures** ... **23**
Bibliography ... **26**

© ISO 2025 – All rights reserved

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).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents. ISO shall not be held responsible for identifying any or all such patent rights.

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 154, *Processes, data elements and documents in commerce, industry and administration*.

This second edition cancels and replaces the first edition (ISO 14533-3:2017), which has been technically revised.

The main changes are as follows:

— terms and definitions have been added in the Clause 3 for clarity;

— the description and the title of tables have been changed in 6.4.2 for clarity.

A list of all parts in the ISO 14533 series can be found on the ISO website.

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 2025 – All rights reserved

Introduction

The purpose of this document is to ensure the interoperability of implementations with respect to long-term signatures that make electronic signatures verifiable in the long term. Long-term signature specifications referenced by each implementation cover CAdES signatures as used in PDF described in ISO 32000-2 (PDF2.0).

© ISO 2025 – All rights reserved

Processes, data elements and documents in commerce, industry and administration — Long-term signature —

Part 3: Profiles for PDF Advanced Electronic Signatures (PAdES)

1 Scope

This document specifies the elements, among those defined in PDF digital signatures (PAdES), that enable verification of a digital signature over a long period of time.

It does not give new technical specifications about the digital signature itself, nor new restrictions of usage of the technical specifications about the digital signatures which already exist.

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

3 Terms and definitions

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
long-term signature
signature that is made verifiable having the ability to maintain its validity status and to get a proof of existence of the associated signed data for a long term by implementing measures to enable the detection of illegal alterations of signature information, including the identification of signing time, the subject of said signature, and validation data

[SOURCE: ISO 14533-1:2022, 3.1]

3.2
profile
rule used to ensure interoperability, related to the optional elements of referenced specifications, the range of values, etc.

3.3
required level
level of requirement for implementing each element constituting a *profile* (3.2)

© ISO 2025 – All rights reserved

3.4
trust anchor
origin of trust provided in the form of a public key *certificate* (3.7) or public key used by the validator to validate an electronic signature, and generally a public key certificate issued by a trusted root *certification authority* (3.6)

[SOURCE: ISO 14533-1:2022, 3.18]

3.5
trusted third party
TTP
security authority or its agent entrusted by another entity in connection with activities related to security

[SOURCE: ISO 14533-1:2022, 3.19]

3.6
certification authority
CA
centre that is entrusted with the development and assignment of public key *certificates* (3.7)

Note 1 to entry: Certification authorities can, at their discretion, develop and assign keys to entities.

3.7
certificate
information on the publicly disclosed key as a part of an asymmetric key pair for an entity, signed by a certification authority to prevent forgery

3.8
PAdES
PAdES digital signature
CAdES signature as used in PDF for which the signer can be identified and any illegal data alteration detected

Note 1 to entry: PDF shall be as defined in ISO 32000-2.

3.9
PAdES-T
PAdES with time
CAdES signature as used in PDF with information to ascertain signing text of the definition

EXAMPLE Signature timestamp, document timestamp.

Note 1 to entry: PDF shall be as defined in ISO 32000-2.

3.10
PAdES-A
archival PAdES
CAdES signature as used in PDF with information that enables the detection of any illegal alterations of information pertaining to the signature, including the subject of the signature and validation data

Note 1 to entry: PDF shall be as defined in ISO 32000-2.

4 Abbreviated terms

EOF end of file

VRI validation-related information

© ISO 2025 – All rights reserved

5 Requirements

5.1 Conformity to PAdES-T

The generation or validation of PAdES-T data conforms to this document, provided that the following requirements are met:

a) all processing of elements whose required level is “Mandatory” in the PAdES-T profile as specified in this document, shall be included;

b) detailed specifications pertaining to the processing of any element whose required level is “Conditional” in the PAdES-T profile, as specified in this document, shall be provided.

5.2 Conformity to PAdES-A

The generation or validation of PAdES-A data conforms to this document provided that the following requirements are met:

a) all processing of elements whose required level is “Mandatory” in the PAdES-A profile as specified in this document, shall be included;

b) detailed specifications pertaining to the processing of any element whose required level is “Conditional” in the PAdES-A profile as specified in this document, shall be provided.

5.3 Conformity to PAdES-DT/DTA

The generation or validation of PAdES-DT and PAdES-DTA data conforms to this document, provided that the requirements of Figures B.1 and B.2 respectively are met. The profile shall be in accordance with Annex B.

5.4 Declaration of conformity

If first-party conformity assessment is used, the implementer shall make a declaration of conformity to this document by disclosing the supplier's declaration of compliance and its attachment (see Annex A) containing a description of implementation status (and the specifications for any elements “Conditional”).

NOTE 1 See ISO/IEC 17050-1.

NOTE 2 Figure 1 shows the positioning of the generation and validation of PAdES-T data and PAdES-A data.

6 Long-term signature profiles

6.1 Definition of PAdES profile and positioning

In order to make electronic signatures verifiable in the long term:

— signing time shall be identifiable;

— any illegal alterations of information pertaining to signatures, including the subject of information and validation data, shall be detectable;

— interoperability shall be ensured.

To meet these requirements, this document defines the following two profiles with respect to PAdES.

a) PAdES-T profile: a profile pertaining to the generation and validation of the signature with a timestamp for signature. The timestamp is stored in a signature timestamp attribute of the signature, or in any subsequent object containing the timestamp, covering the signature. The subsequent object is a document timestamp or a signature with the signature timestamp attribute.

© ISO 2025 – All rights reserved