



DPC: 24/30490646 DC

BSI Group Headquarters

389 Chiswick High Road London W4 4AL

Tel: +44 (0)20 8996 9000

Fax: +44 (0)20 8996 7400

www.bsigroup.com

Date: 07 August 2024

Origin: International

Latest date for receipt of comments: 30 September 2024

Project No. 2024/01023

Responsible committee: IST/47/-/3 eBusiness

Interested committees:

Title: Draft BS ISO 14533-3 Processes, data elements and documents in commerce, industry and administration - Long term signature. Part 3: profiles for PDF Advanced Electronic Signatures (PADES).

Please notify admin.start@bsigroup.com if you are aware of any keywords that might assist in clarifying or identifying the standard or of the content of this standard:

- i) has any issues related to 3rd party IPR, patent or copyright
- ii) affects other national standard(s)
- iii) requires additional national guidance or information

WARNING: THIS IS A DRAFT AND MUST NOT BE REGARDED OR USED AS A BRITISH STANDARD. THIS DRAFT IS NOT CURRENT BEYOND 30 September 2024

This draft is issued to allow comments from interested parties; all comments will be given consideration prior to publication. No acknowledgement will normally be sent. **See overleaf for information on the submission of comments.**

No copying is allowed, in any form, without prior written permission from BSI except as permitted under the Copyright, Designs and Patent Act 1988 or for circulation within a nominating organization for briefing purposes. Electronic circulation is limited to dissemination by e-mail within such an organization by committee members.

Further copies of this draft may be purchased from BSI Shop <http://shop.bsigroup.com> or from BSI Customer Services, Tel: +44(0) 20 8996 9001 or email cservices@bsigroup.com. British, International and foreign standards are also available from BSI Customer Services.

Information on the co-operating organizations represented on the committees referenced above may be obtained from <https://standardsdevelopment.bsigroup.com/>.

Introduction

This draft standard is based on national and international discussions. Your comments on this draft are invited and will assist in the preparation of the consequent standard.

For international standards, comments will be reviewed by the relevant UK national committee before sending the consensus UK vote and comments to the international committee, which will then decide appropriate action. If the international standard is approved, it is usual for the text to be published as a British Standard.

For national standards, comments will be reviewed by the relevant UK national committee and the resulting standards published as a British Standard.

UK Vote

Please indicate whether you consider the UK should submit a negative (with supporting technical reasons) or positive vote on this draft. Please indicate if you are aware of any reason why this draft standard should not be published as a British Standard.

Submission of Comments

- **Annotated drafts are not acceptable and will be rejected.**
- All comments should be submitted online at <https://standardsdevelopment.bsigroup.com/>. You will need to register in order to comment.

Template for comments and secretariat observations

Date: xx/xx/20xx	Document: ISO/DIS xxxx
------------------	------------------------

1	2	(3)	4	5	(6)	7
MB	Clause No./ Subclause No./Annex (e.g. 3.1)	Paragraph/ Figure/Table/Note	Type of comment	Comment (justification for change) by the MB	Proposed change by the MB	Secretariat observations on each comment submitted
	3.1	Definition 1	ed	Definition is ambiguous and needs clarifying.	Amend to read '...so that the mains connector to which no connection...'	
	6.4	Paragraph 2	te	The use of the UV photometer as an alternative cannot be supported as serious problems have been encountered in its use in the UK.	Delete reference to UV photometer.	



DRAFT International Standard

ISO/DIS 14533-3

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

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

ICS: 35.240.63

ISO/TC 154

Secretariat: **SAC**

Voting begins on:
2024-08-07

Voting terminates on:
2024-10-30

This document is circulated as received from the committee secretariat.

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENTS AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

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.

Reference number
ISO/DIS 14533-3:2024(en)

Full document details: 24/30490646 DC

© ISO 2024  **Documents**
Document Sharing Hub



COPYRIGHT PROTECTED DOCUMENT

© ISO 2024

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 and symbols	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 (normative) Supplier's declaration of conformity and its attachment	14
Annex B (normative) The profile for using only timestamp	19
Annex C (normative) Structure of timestamp token	21
Annex D (informative) Applying PAdES using CMS signatures	23
Annex E (informative) Examples of multiple signatures	24
Bibliography	27

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 are added in the [Clause 3](#) for clarity.
- The description and the title of tables are 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.

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).

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 14533-1, *Processes, data elements and documents in commerce, industry and administration — Long term signature — Part 1: Profiles for CMS Advanced Electronic Signatures (CAAdES)*

ISO 32000-2, *Document management — Portable document format — Part 2: PDF 2.0*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in Part 1 of ISO 14533 and the following apply.

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 and has 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 14533-1:2020]

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

3.4

trust anchor

origin of trust provided in the form of a public key certificate 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

[SOURCE: ISO 14533-1:2020]

3.5

trusted third party

TTP

security authority or its agent entrusted by another entity in connection with activities related to security

[SOURCE: ISO 14533-1:2020]

3.6

certification authority

CA

centre that is entrusted with the development and assignment of public key certificates

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 digital signature (PAdES)

CAdES signatures as used in PDF defined in ISO 32000-2 for which the signer can be identified and any illegal data alteration detected

3.9

PAdES with time

PAdES-T

CAdES signatures as used in PDF defined in ISO 32000-2 with information to ascertain signing text of the definition

EXAMPLE Signature Timestamp, Document Timestamp.

3.10

Archival PAdES

PAdES-A

CAdES signatures as used in PDF defined in ISO 32000-2 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

4 Abbreviated terms and symbols

The following symbols are used for the “required level”:

- C: Conditional
- M: Mandatory
- O: Optional
- P: Prohibited (creation or modification)

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. See [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 17050-1:2004.

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, and
- 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.