INTERNATIONAL STANDARD

ISO 14533-3

First edition
2017-09

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

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

Processus, éléments d'informations et documents dans le commerce, l'industrie et l'administration — Profils de signature à long terme — Partie 3: Profils de signature à long terme pour les signatures électroniques avancées PDF (PAdES)

Reference number
ISO 14533-3:2017(E)

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

Contents

Page

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 on 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 the following URL: 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*.

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

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 PDF Advanced Electronic Signatures (PAdES) developed by the European Telecommunications Standards Institute (ETSI).

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

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

1 Scope

This document specifies the elements, among those defined in PDF Advanced Electronic 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 profiles — Part 1: Long term signature profiles for CMS Advanced Electronic Signatures (CAdES)*

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 ISO 14533-1 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at http://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1
advanced electronic signature
electronic signature which is uniquely linked to the signatory, is capable of identifying the signatory, is created using electronic signature creation data that the signatory can, with high level of confidence, use under his sole control, and is linked to the data signed therewith in such a way that any subsequent change in the data is detectable

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 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 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 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 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.

b) PAdES-A profile: a profile pertaining to the generation and validation in the long-term availability and integrity of the validation data that protects the PAdES-T data, including validation data from any illegal alterations.

Figure 1 shows the relation between the PAdES-T data and the PAdES-A data.

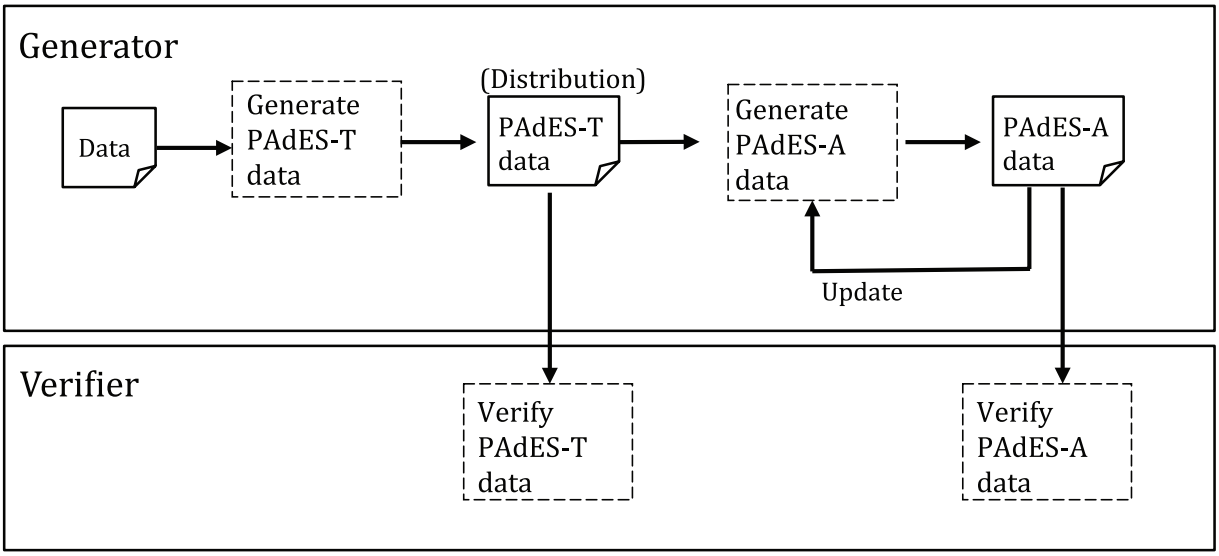

Figure 1 — Relation between the PAdES-T data and the PAdES-A data

6.2 Representation of the required level

This document defines the following representation methods for the required level (as a profile) of each element constituting PAdES-T data and PAdES-A data.

a) Mandatory (M): Elements whose required level is “Mandatory” shall be implemented without fail. If such an element has optional sub-elements, at least one sub-element shall be selected. Any element whose required level is “Mandatory” and which is one of the sub-elements of an optional element shall be selected whenever the optional element is selected.

b) Optional (O): Elements whose required level is “Optional” may be implemented at the discretion of the implementer.

c) Conditional (C): Elements whose required level is “Conditional” may be implemented at the discretion of the implementer, provided that detailed specifications for the processing thereof are provided separately.

d) Prohibited (P): Elements whose required level is ‘Prohibited’ shall not be created or modified, but may be read.

6.3 Standard for setting the required level

The required level of each element constituting PAdES-T data and PAdES-A data shall be set in accordance with the following requirements:

a) The required level shall be “Mandatory” for elements whose required level is “Mandatory” in the definition of PAdES, and for elements that are necessary for the generation and validation of long-term signatures. The elements whose required level is “Optional” in the definition of PAdES are defined as “Mandatory”, “Optional” or “Conditional”.

b) The required level shall be “Conditional” for externally defined elements.

EXAMPLE 1 OtherCertificateFormat.

c) The required level shall be “Conditional” for elements intended to interact with a certain application.

EXAMPLE 2 CommitmentType.

d) The required level shall be “Conditional” for elements with an operation-dependent factor.

EXAMPLE 3 Attribute certificate; time mark.

NOTE The archiving-type timestamp defined in ISO/IEC 18014-2 is included in “Time mark or other method.”

e) The required level shall be “optional” for elements only containing reference information.

6.4 PAdES-T profile

6.4.1 General

The PAdES-T profile is defined as the form of an electronic signature, of which the signature value is protected by any subsequent object containing trusted evidence as a proof of existence (e.g. Document timestamp).

The PAdES-T is extended from the PAdES using CAdES signatures specified in 6.4.2. The required levels of constituent elements of the PAdES using CAdES signatures are also specified in 6.4.2.

The following three types are defined as forms of the PAdES-T profile.

— PAdES-T by Document timestamp;

— PAdES-T by Signature timestamp Attribute;

— PAdES-T by Subsequent Signature with Signature timestamp Attribute.

These forms are shown in Figure 2 to 4.

The required levels of PAdES-T profile are specified in 6.4.3.

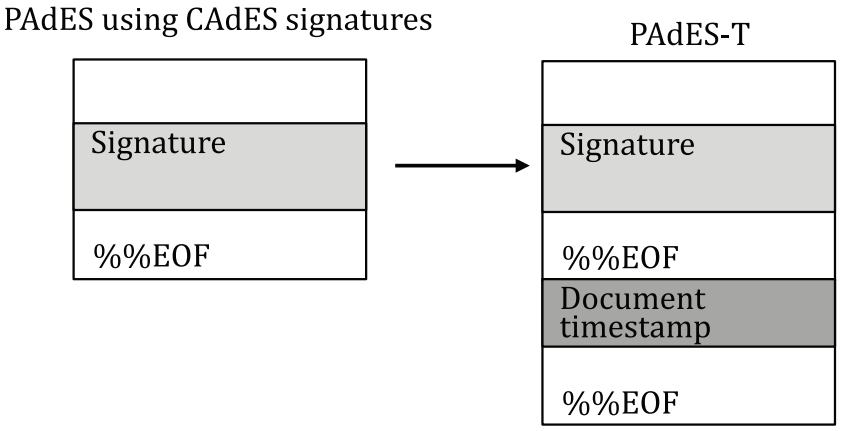

Figure 2 — PAdES-T Profile by Document timestamp

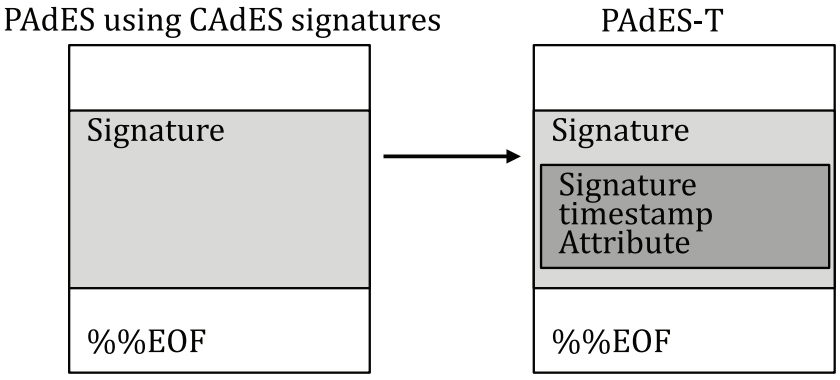

Figure 3 — PAdES-T Profile by Signature timestamp Attribute

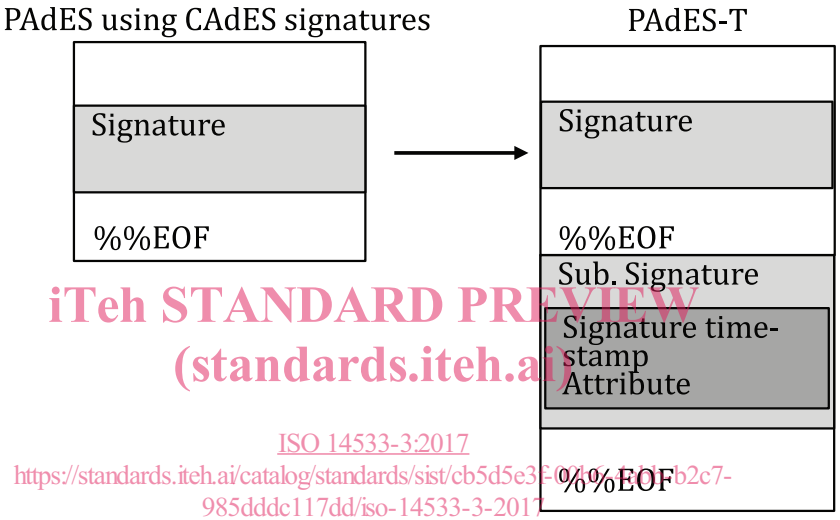

Figure 4 — PAdES-T Profile by Subsequent Signature with Signature timestamp Attribute

6.4.2 PAdES using CAdES signatures profile

Table 1 specifies the required levels of entries that constitute the Signature Directory of the PAdES using CAdES signatures profile. The element which has not been indicated is set to C (Conditional).

Table 1 — Signature Dictionary of PAdES using CAdES signatures

Entry	Required level	Value
Type	O	Sig
Filter	M	
SubFilter	M	ETSI.CAdES.detached [a]
Contents	M	See Table 2
ByteRange	M	
M	M [b]	
Cert	P	

[a] See also Annex D.

[b] Even if a signature does not contain M Entry, a signature validation application shall not consider this signature invalid. Time of M Entry is not basically used to validate certificates. If this information is used for validation, it is necessary to define clearly a usage of this information. (e.g. describing a usage in a signature policy).

Table 1 *(continued)*

Entry	Required level	Value
Location	O	
Reason	O	
ContactInfo	O	

[a] See also Annex D.

[b] Even if a signature does not contain M Entry, a signature validation application shall not consider this signature invalid. Time of M Entry is not basically used to validate certificates. If this information is used for validation, it is necessary to define clearly a usage of this information. (e.g. describing a usage in a signature policy).

Table 2 specifies the required levels of elements that constitute the ContentInfo in the signature data.

Table 2 — ContentInfo in signature

Element	Required level	Value
ContentType	M	id-signedData
Content	M	See Table 3

Table 3 specifies the required levels of elements that constitute the SignedData in the signature data. A DER-encoded SignedData object as specified in cryptographic message syntax (CMS) shall be included as the PDF signature in the entry with the key Content of the signature dictionary, as described in ISO 32000-2.

Table 3 — SignedData in signature

Element	Required level
CMSVersion	M
DigestAlgorithmIdentifiers	M
EncapsulatedContentInfo	M
– eContentType	M
– eContent	O
CertificateSet (Certificates)	M
– Certificate	M [a]
– AttributeCertificateV2	P
– OtherCertificateFormat	C
RevocationInfoChoices (crls)	O
– CertificateList	O
– OtherRevocationInfoFormat	C
SignerInfos	M [b]
– signerInfo	M

[a] At least a signature generation application shall contain a signer certificate for interoperability. Even if a signature does not contain this element, a signature validation application shall not consider this signature invalid.

[b] Only a single signerInfo shall be present in PDF signature.

Table 4 specifies the required levels of elements that constitute the SignerInfo in the signature data.

Table 4 — SignerInfo in signature

Element	Required level
CMSVersion	M
SignerIdentifier	M
– IssuerAndSerialNumber	O