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.

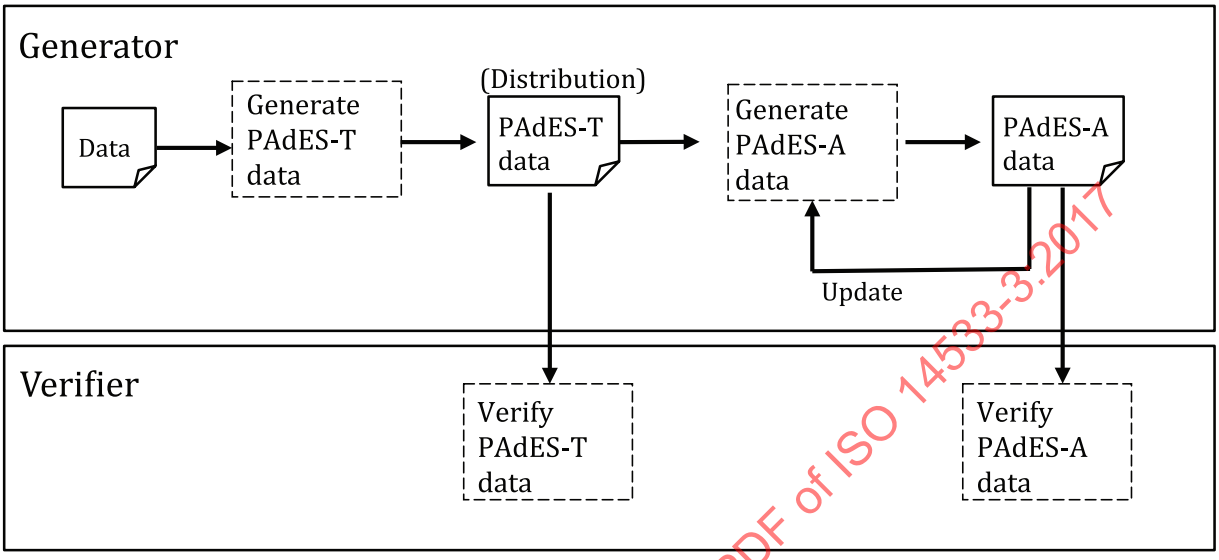

Figure 1 — Relation between the PAdES-T data and the PAdES-A data

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.

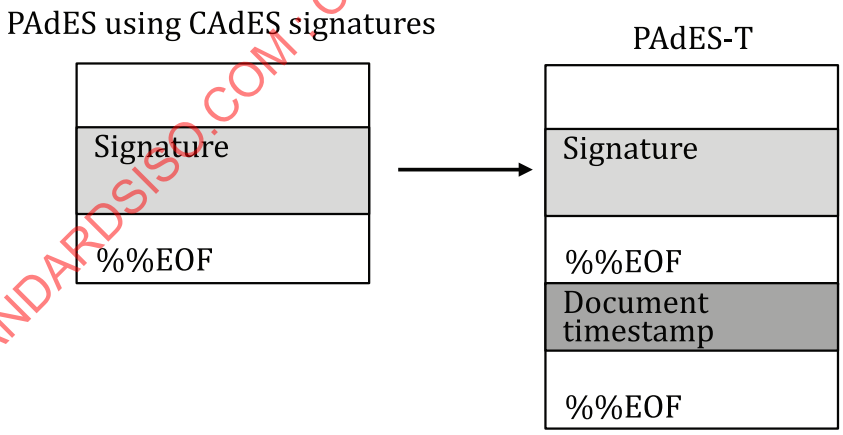

Figure 2 — PAdES-T Profile by Document timestamp

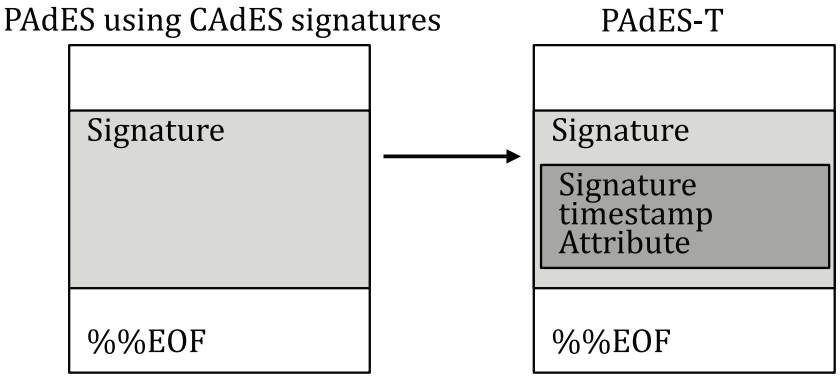

Figure 3 — PAdES-T Profile by Signature timestamp Attribute

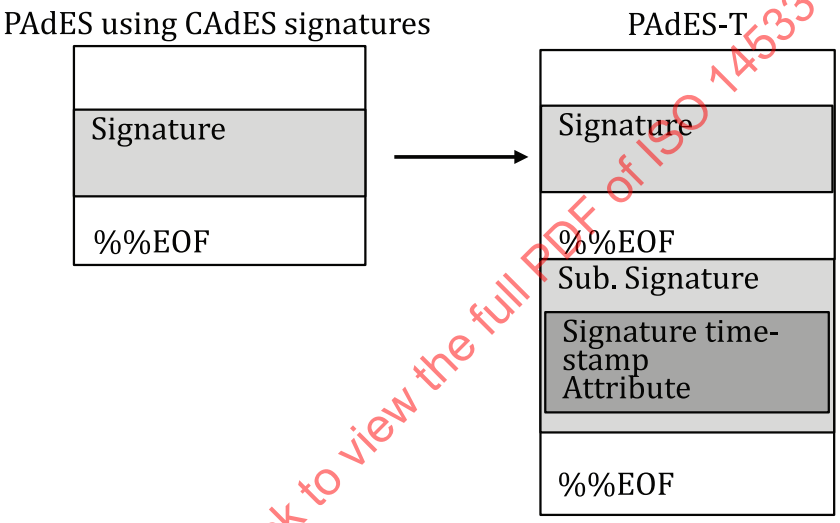

Figure 4 — PAdES-T Profile by Subsequent Signature with Signature timestamp Attribute

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

Table 4 *(continued)*

Element	Required level
– SubjectKeyIdentifier	O
DigestAlgorithmIdentifier	M
SignedAttributes	M
SignatureAlgorithmIdentifier	M
SignatureValue	M
UnsignedAttributes	O

Table 5 specifies the required levels of elements that constitute the Signed Attributes. The element which has not been indicated is set to C (Conditional).

Table 5 — Signed Attribute in signature

Element	Required level
ContentType	M
MessageDigest	M
SigningCertificateReference	M
– ESS SigningCertificate	O
– ESS SigningCertificateV2	O [a]
– OtherSigningCertificate	C
SignaturePolicyIdentifier	C [b]
CommitmentTypeIndication	C [b]
SignerIdentifier	C
ContentTimestamp	C
SigningTime	P
ContentReference	P
ContentIdentifier	P
ContentHints	P
SignerAttribute	C [c]
SignerLocation	O [d]

[a] When a signature which complies with the PAdES using CAdES signatures is generated, the attribute of signingCertificateV2 shall be present in Signed Attributes.

[b] See ISO 32000-2:2017, 12.8.3.4.4.

[c] See ISO 32000-2:2017, 12.8.3.4.3.

[d] Either SignerLocation attribute or Location entry in Table 1 may be used.

Table 6 specifies the required levels of elements that constitute the Unsigned Attributes. The element which has not been indicated is set to C (Conditional).

Table 6 — Unsigned Attributes in signature

Element	Required level
CounterSignature	P

6.4.3 Timestamp of PAdES-T profile

See Table 7.

a) PAdES-T profile by Document timestamp.

The PAdES-T profile by Document timestamp is defined as an extended form of the PAdES using CAdES signatures profile to which the Document timestamp dictionary is added.

b) PAdES-T profile by Signature Timestamp Attribute

The PAdES-T profile by Signature Timestamp Attribute is defined as an extended form to which the Signature Timestamp Attribute is added.

c) PAdES-T profile by Subsequent Signature with Signature Timestamp Attribute

The PAdES-T profile by Subsequent Signature with Signature Timestamp Attribute is defined as an extended form of the PAdES using CAdES signatures profile to which the Subsequent Signature Dictionary is added, containing the signature with the Signature Timestamp Attribute.

The time value of PAdES-T shall be the time value of the oldest valid timestamp covering the signature value according to point a), b) or c).

Table 7 — Timestamp of PAdES-T profile

Element	Required level
timestamp for signature	M
– Document timestamp dictionary	O
– Signature timestamp Attribute (unsigned attributes in signature data)	O
– Subsequent Signature with a Signature timestamp Attribute (unsigned attributes in signature data)	O
The profile of timestamp token is described in Annex C.	

6.5 PAdES-A profile

6.5.1 General

The required levels of constituent elements of PAdES-A profile are specified in 6.5.2 to 6.5.7.

6.5.2 Structure of the PAdES-A profile

The PAdES-A profile is defined as the form of an electronic signature of which the PDF objects are protected by trusted evidence as a proof of existence (e.g. Document timestamp). The PDF objects contain the following objects:

— Data to be signed;

— Signature value;

— Trusted evidence which protects the signature value;

— Trusted evidences for PDF objects in the past;

— Validation information updated (thisUpdate of CRL or OCSP response) after the time value of PAdES-T of signature value and trusted evidences.

NOTE See Rec. ITU-T X.509, ISO/IEC 9594-8 or IETF RFC 6960.

The PAdES-A profile is an extended form of the PAdES-T profile to which the elements specified in Table 8 are added. The PAdES-A enables the detection of any illegal alterations of information pertaining to the signature, including the subject of the signature and validation data.

Table 8 — Elements of PAdES-A profile

Element	Required level
Document Security Store (DSS) Dictionary	M
Document timestamp Dictionary	M

6.5.3 Document Security Store Dictionary

The requirements of entries that constitute the Document Security Store (DSS) dictionary are specified in ISO 32000-2.

The DSS may contain the certificates and the revocation information which are used to validate the signatures, the signature timestamps, and the Document timestamps appended prior to the DSS dictionary.

6.5.4 Signature VRI Dictionary

The requirements of entries that constitute the Signature VRI Dictionary are specified in ISO 32000-2.

6.5.5 Document timestamp

Table 9 shows the Signature Dictionary of Document timestamps.

Table 9 — Signature Dictionary of DocTimeStamp

Entry	Required level	Value
Type	M	DocTimeStamp
Filter	M	
SubFilter	M	ETSI.RFC3161
Contents	M	TimeStampToken [a]
ByteRange	M [b]	
Reference	P	
Changes	P	
Name	P	
M	P	
Cert	P	
Location	P	
Reason	P	
ContactInfo	P	
R	P	
V	O	0
Prop_Build	O	
Prop_AuthTime	P	
Prop_AuthType	P	

[a] As specified in RFC 3161.

[b] The ByteRange shall cover the entire file, including the signature dictionary but excluding the Contents value.

The Document timestamp shall be affixed after the DSS dictionary is appended. The requirements of entries that constitute the Document timestamp are specified in ISO 32000-2. The profile of timestamp token is described in Annex C.

6.5.6 Updating PAdES-A

In order to ensure the validity of the signatures and/or the timestamps in the long term, a new Document timestamp shall be affixed at a time when the cryptographic algorithms used in the latest Document timestamp are considered reliable, and the certificates of the Document timestamp are not expired. The following steps shall be performed:

a) The set of certificates and revocation information used to validate the latest Document timestamp are obtained.

b) The set of certificates and revocation information are stored in the PDF file as the stream objects. The DSS dictionary that contains the references to these objects is appended, and if required, the VRI is appended.

c) The Document timestamp is affixed to the PDF file obtained in step b).

6.5.7 Validation Data for Signature and Timestamp

The validation data is a set of certificates up to the trust anchor and revocation information to be used for validation of signatures and timestamps. The validation data may be stored with the PAdES signature as described in Table 10. When not stored with the PAdES signature, validation data shall be stored by another secure means including, but not limited to, storage by a certification authority (CA) as a trusted third party (TTP) or by timestamping authority (TSA).

Table 10 — Elements of storing validation data

Type of validation data	Elements of storing validation data	Required level	Preferred order
Validation data for signatures	Fields inside the SignedData of the signature	O	
	Stream objects referred by DSS	O	1
	Stream objects referred by VRI	O	2
Validation data for timestamp token of signature timestamp attribute	Fields inside the SignedData of the timestamped signature	O	
	Fields inside the signature timestamp	O [a]	
	Stream objects referred by DSS	O	1
	Stream objects referred by VRI	O	2
Validation data for timestamp token of Document timestamp	Fields inside the SignedData of the timestamped signature	P	
	Fields inside the Document timestamp	O [a]	
	Stream objects referred by DSS	O	1
	Stream objects referred by VRI	O	2

[a] Revocation information should be stored using DSS or VRI.

6.6 Multiple signatures

6.6.1 General

Multiple signatures may be appended to a PDF file by using incremental update. In the case of multiple signatures, the conformity of a whole PDF file is defined as follows:

— When all signatures in a PDF file conform to the PAdES-A profile, this PDF file conforms to the PAdES-A profile.

— When signatures conforming to the PAdES-T profile and signatures conforming to the PAdES-A profile coexist in a PDF file, this PDF file conforms to the PAdES-T profile.

The examples of multiple signatures are described in Annex E.

6.6.2 Timestamp for multiple signatures

In the case of applying PAdES-T to multiple signatures, even without attaching respective timestamps to the signatures, a timestamp of PAdES-T can also be applied to all of the signatures. Figure 5 shows an example of a timestamp for multiple signatures by Document timestamp. Because this Document timestamp is generated from byte range including both Signature1 and Signature2, it provides a proof of existence of both signatures.

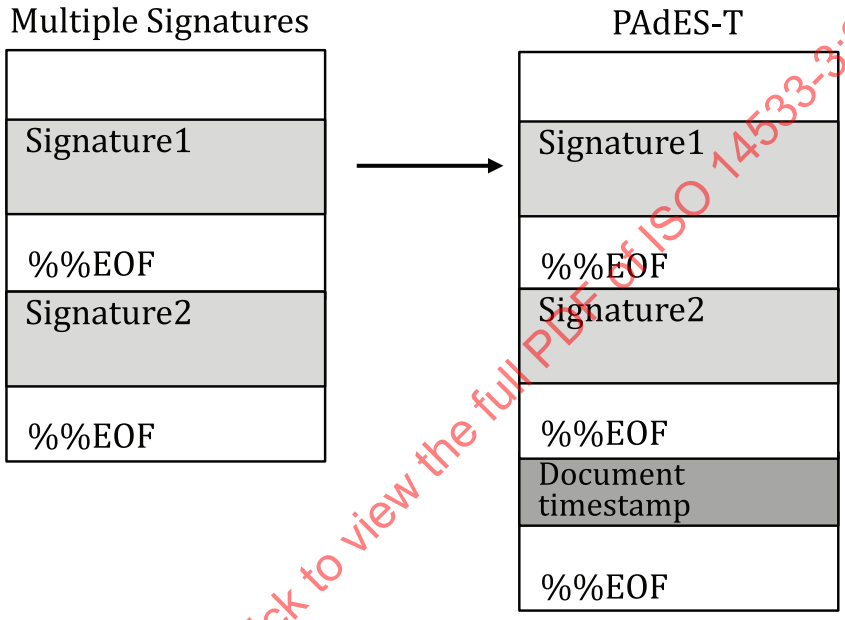

Figure 5 — Timestamp for multiple signatures by Document timestamp

Figure 6 describes an example of timestamp for multiple signatures by Signature Timestamp Attribute. This Signature TimeStamp Attribute in Signature2 is generated from the signature value of Signature2, and the signature value of Signature2 is generated from byte range including Signature1. Therefore, this Signature TimeStamp Attribute logically protects both Signature2 and Signature1. This Signature TimeStamp Attribute can be used as timestamp for both signatures.

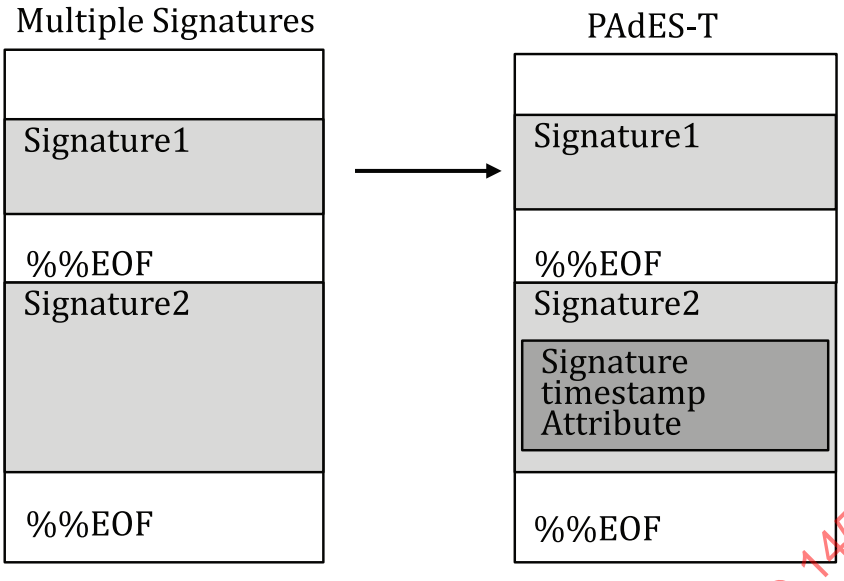

Figure 6 — Timestamp for multiple signatures by Signature Timestamp Attribute

Unless all signatures and a timestamp can be generated immediately, and time difference between all signatures and a timestamp is acceptable, a timestamp of PAdES-T shall be generated for each signature immediately after signing.

Annex A
(normative)

Supplier's declaration of conformity and its attachment

A.1 General

This annex specifies the form of the supplier's declaration of conformity to the PAdES long-term signature profile.

A.2 Form of the supplier's declaration of conformity

Supplier's declaration of conformity to the long term signature profile
Number:
Issuer's name:
Issuer's address:
Object of declaration:
The object of the declaration described above is in conformity with the requirement of the following long-term signature profiles.
PAdES-T profile and/or **PAdES-A profile**
PAdES-DT profile (see Clause B.2) and/or **PAdES-DTA profile** (See Clause B.3)
The implemented elements are as specified in Clause A.3 below.
Additional information:
(The results of operation checks, etc. may be inserted here.)
Signed for and on behalf of:
(Place and date of issue)
(Name, title)

A.3 Form of the attachment to the supplier's declaration of conformity

A.3.1 General

The attachment to the supplier's declaration of conformity shall contain the items specified in A.3.2 to A.3.9 (see Tables A.1 to A.13).

A.3.2 Version number of standard to be referenced

A.3.3 Scope of profile implementation

Table A.1 — Profile Implementation

Profile identifier	Generator	Verifier
PAdES-T		
PAdES-A		
PAdES-DT		
PAdES-DTA		

A.3.4 Conformity to the PAdES-T profile

Table A.2 — PAdES-T Profile Implementation

Profile identifier	Generator	Verifier
PAdES-T profile by Document timestamp		
PAdES-T profile by Signature timestamp Attribute		
timestamp for multiple signatures		
– by Document timestamp		
– by Signature timestamp		
– by Subsequent Signature with a Signature timestamp		

Table A.3 — Signature Dictionary

Entry	Required level	Generator	Verifier
Type	O		
Filter	M		
SubFilter	M		
Contents	M		
ByteRange	M		
M	M		
Cert	P		
Location	O		
Reason	O		
ContactInfo	O		

Table A.4 — ContentInfo in signature data

Element	Required level	Generator	Verifier
ContentType	M		
Content	M		

Table A.5 — SignedData in signature data

Element	Required level	Generator	Verifier
CMSVersion	M		
DigestAlgorithmIdentifiers	M		
EncapsulatedContentInfo	M		
– eContentType	M		

Table A.5 *(continued)*

Element	Required level	Generator	Verifier
– eContent	O		
CertificateSet (Certificates)	M		
– Certificate	M		
– AttributeCertificateV2	P		
– OtherCertificateFormat	C		
RevocationInfoChoices (crls)	O		
– CertificateList	O		
– OtherRevocationInfoFormat	C		
SignerInfos	M		
– signerInfo	M		

Table A.6 — SignerInfo in signature data

Element	Required level	Generator	Verifier
CMSVersion	M		
SignerIdentifier	M		
– IssuerAndSerialNumber	O		
– SubjectKeyIdentifier	O		
DigestAlgorithmIdentifier	M		
SignedAttributes	M		
SignatureAlgorithmIdentifier	M		
SignatureValue	M		
UnsignedAttributes	O		

Table A.7 — Signed Attributes in signature data

Element	Required level	Generator	Verifier
ContentType	M		
MessageDigest	M		
SigningCertificateReference	M		
– ESS SigningCertificate	O		
– ESS SigningCertificateV2	O		
– otherSigningCertificate	C		
SignaturePolicyIdentifier	C		
CommitmentTypeIndication	C		
SignerIdentifier	C		
ContentTimestamp	C		
SigningTime	P		
ContentReference	P		
ContentIdentifier	P		
ContentHints	P		
SignerAttribute	C		
SignerLocation	O		

Table A.8 — Unsigned Attributes in signature data

Element	Required level	Generator	Verifier
CounterSignature	P		
timestamp for signature	O		
– Signature timestamp token	O		

A.3.5 Conformity to the PAdES-A profile

Table A.9 — Elements of PAdES-A profile

Entry	Required level	Generator	Verifier
Document Security Store (DSS) Dictionary	M		
Document timestamp dictionary	M		

Table A.10 — Validation information store

Type of validation data	Elements of storing validation data	Required level	Generator	Verifier
Validation data for the signature	Fields inside the SignedData of the signature	O [a]		
	Stream object s referred by DSS	O		
	Stream objects referred by VRI	O		
Validation data for the timestamp token of the Signature timestamp attribute	Fields inside the SignedData of the times-tamped signature	O		
	Fields inside the Signature timestamp	O [a]		
	Stream object s referred by DSS	O		
	Stream objects referred by VRI	O		
Validation data for times-tamp token of Document timestamp	Fields inside the SignedData of the times-tamped signature	P		
	Fields inside the Document timestamp	O [a]		
	Stream object s referred by DSS	O		
	Stream objects referred by VRI	O		

[a] The revocation information should be stored using DSS or VRI.

A.3.6 Conformity to the PAdES-DT profile (see Clause B.2)

Table A.11 — The elements of PAdES-DT profile

Entry	Required level	Generator	Verifier
Document timestamp dictionary	M		

A.3.7 Conformity to the PAdES-DTA profile (see Clause B.3)

Table A.12 — The elements of PAdES-DTA profile

Entry	Required level	Generator	Verifier
Document Security Store (DSS) Dictionary	M		
Document timestamp dictionary	M		

A.3.8 Specifications to be referenced by elements “Conditional”

Table A.13 — “Conditional” elements

Number	Element name	Referenced specification
1.		
2.		

A.3.9 Remarks

Annex B
(normative)

The profile for using only timestamp

B.1 General

The Document timestamp can be applied to a PDF file that does not contain electronic signature data. This Document timestamp functions as a proof of existence of a PDF file.

B.2 PAdES-DT profile

B.2.1 General

The PAdES-DT profile is defined as a PDF file that contains a dictionary of a Document timestamp, but not a signature. The data conforming to the PAdES-DT profile shall meet the following:

— The data does not contain a signature dictionary (The value of Type is Sig).

— The data contains Document timestamp dictionaries (The value of Type is DocTimeStamp).

The PAdES-DT data may contain more than one Document timestamp. Figure B.1 shows the form of the PAdES-DT data.

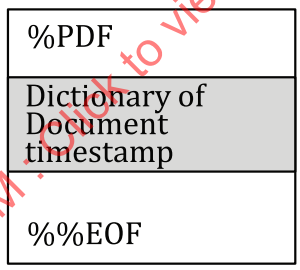

Figure B.1 — Structure of PAdES-DT

B.2.2 Dictionary of Document timestamp

The requirements of elements that constitute the dictionary of the Document timestamp are specified in ISO 32000-2.

B.3 PAdES-DTA profile

The PAdES-DTA profile is defined as the form that enables the detection of any illegal alterations of information pertaining to the Document timestamps, including the subject of the timestamp and validation data. The PAdES-DTA data is extended from the PAdES-DT data. The requirements are the same as the PAdES-A profile, except that the data does not contain the signature dictionary (Type: Sig).

Figure B.2 shows the relation between the PAdES-DT data and the PAdES-DTA data.

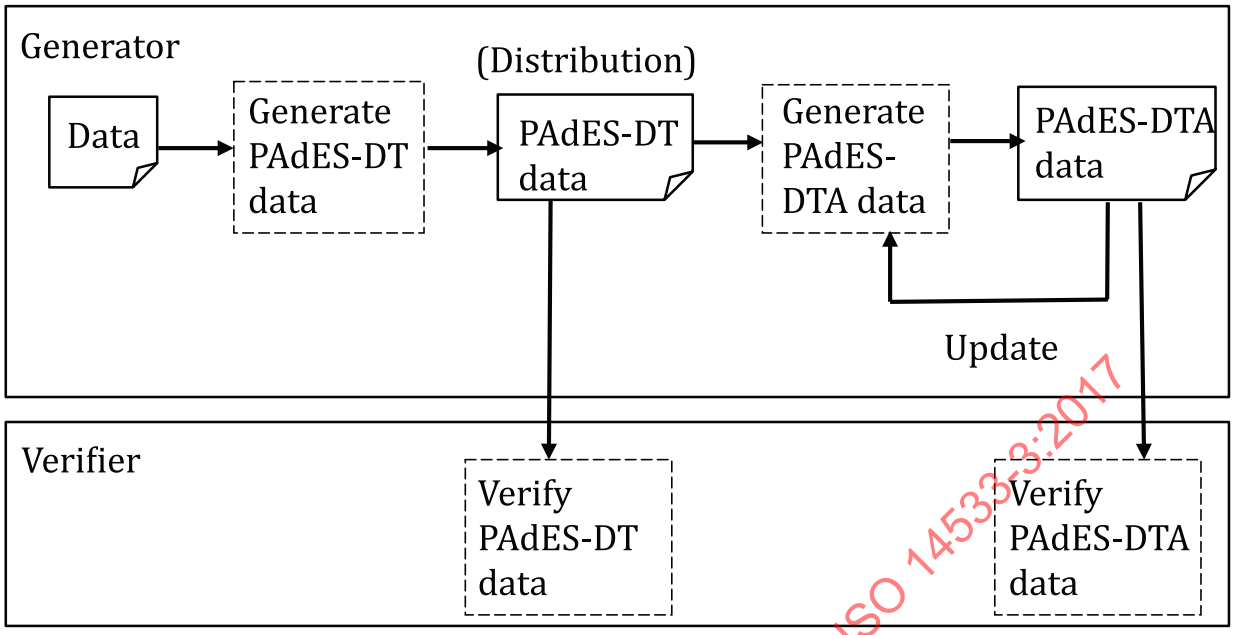

Figure B.2 — Relation between the PAdES-DT data and the PAdES-DTA data

Annex C
(normative)

Structure of timestamp token

C.1 General

This annex specifies the requirements for the structure of a timestamp token in a long-term signature.

C.2 Normative specifications

The signature timestamp token and "the long-term Availability and integrity of the validation data" archive timestamp token in this document shall conform to CMS, TSP, CAdES.

NOTE Timestamp Protocol (TSP) is defined in IETF RFC 3161.

C.3 Required level of constituent elements

The required level of each element of the signature timestamp token and "the long-term Availability and integrity of the validation data" archive timestamp token shall be as specified in Table C.1.

Table C.1 — Required level of each element of the timestamp token

Entry	Required level	Value
ContentType	M	id-signedData
Content	M	Signed Data
– CMSVersion	M	
– DigestAlgorithmIdentifiers	M	
– EncapsulatedContentInfo	M	
– eContentType	M	id-ct-TSTInfo
– eContent	M	DER-encoded value of TSTInfo
– CertificateSet (Certificates)	O	
– Certificate	M	At least a signer certificate of TSA shall be provided.
– AttributeCertificateV1	O	
– AttributeCertificateV2	O	
– OtherCertificateFormat	O	
– RevocationInfoChoices (crls)	O	
– CertificateList	O	
– OtherRevocationInfoFormat	O	
– SignerInfos	M	
– SignerInfo	M	
– CMSVersion	M	
– SignerIdentifier	M	
– IssuerAndSerialNumber	O	

[a] The ESSSigningCertficate v2 shall be used when another hash algorithms than SHA-1 is used and should be used when a new TimeStampToken is obtained.

Table C.1 *(continued)*

Entry	Required level	Value
– SubjectKeyIdentifier	O	
– DigestAlgorithmIdentifier	M	
– SignedAttributes	M	
– ContentType	M	id-ct-TSTInfo
– MessageDigest	M	
– SigningCertificateReference	M	
– ESS SigningCertificate	O	
– ESS SigningCertificate v2	O [a]	
– OtherSigningCertificate	C	
– SignatureAlgorithmIdentifier	M	
– SignatureValue	M	
– UnsignedAttributes	O	
– CompleteCertificateReferences	O	
– CompleteRevocationReferences	O	
– CompleteRevRefs CRL	O	
– CompleteRevRefs OCSP	O	
– CertificateValues	O	
– CertificateValues	O	
– Storage of the certificate by CA	C	
– RevocationValues	O	
– CertificateList	O	
– BasicOCSPResponse	O	
– OtherRevVals	C	

[a] The ESSSigningCertficate v2 shall be used when another hash algorithms than SHA-1 is used and should be used when a new TimeStampToken is obtained.