ISO/TC 154 "Processes, data elements and documents in commerce, industry and administration"
Secretariat: **SAC**
Committee Manager: **Zhang Jianfang Mr**

ISO 14533-2 for publication

Document type	Related content	Document date	Expected action
Project / Draft	Project: ISO/DIS 14533-2	2021-04-28	

Description

ISO/DIS 14533-2 ballot was approved and the update draft will be directly into IS publication as per N1206(Form 13). The document is the final submission to ISO/CS for publication.

Reference number of project: ISO 14533-2 : 2021

Date: 2021-04-27

Identification of Committee: ISO/TC 154

Secretariat of Committee: SAC

Processes, data elements and documents in commerce, industry and administration — Long term signature — Part 2: Profiles for XML Advanced Electronic Signatures (XAdES)

ISO copyright office

CP 401 • Ch. de Blandonnet 8

CH-1214 Vernier, Geneva

Phone: +41 22 749 01 11

Fax: +41 22 749 09 47

Email: copyright@iso.org

Website: www.iso.org

Published in Switzerland

Contents

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 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 *[or Project Committee]* ISO/TC *[or ISO/PC]* ###, *[name of committee]*, Subcommittee SC ##, *[name of subcommittee],* in collaboration with the European Committee for Standardization (CEN) Technical Committee CEN/TC ###, *[name of committee],* in accordance with the Agreement on technical cooperation between ISO and CEN (Vienna Agreement).

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 14533-2:2012), which has been technically revised.

The main changes compared to the previous edition are as follows:

— In first edition (ISO 14533-2:2012), XAdES was an abbreviated term for ‘XML Advanced Electronic Signature’. In this document, XAdES becomes a proper noun and is used as ‘XAdES digital signature’.

— Supports XML namespace XAdES 1.4.1 elements.

— XAdES-A profile level was divided and explained as XAdES-X-Long form level.

— Described comparison with European EN in Annex C, "(informative) Differences of required level between European EN and ISO specification".

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 digital signatures verifiable for a long term. Long term signature specifications referenced by each implementation cover XAdES digital signatures developed by the European Telecommunications Standards Institute (ETSI).

ETSI EN 319 132 specifies data structures and core elements for XAdES digital signature. This document profiles ETSI EN 319 132 specification for international long term signature interoperability. ETSI EN 319 132 specification provides definitions of data structures, data elements and their usage in detail. To maintain consistency with ETSI EN 319 132 specification, this document avoids quoting and redefining those components defined in ETSI EN 319 132 specification.

In the first edition (ISO 14533-2:2012), XAdES was an acronym for 'XML Advanced Electronic Signature'. In this second edition (ISO 14533-2:2021), XAdES is used as a proper noun and 'XML Advanced Electronic Signature' is changed to 'XAdES Digital Signature' in line with the definition change of ETSI from TS to EN. But still used in this document title.

Processes, data elements and documents in commerce, industry and administration — Long term signature — Part 2: Profiles for XML Advanced Electronic Signatures (XAdES)

1 Scope

This document specifies the elements, among those defined in XAdES digital signatures, 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.

NOTE XAdES digital signatures is the extended specification of "XML-Signature Syntax and Processing" used widely.

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)*

ETSI EN 319 132-2[1], *XAdES digital signatures Part 2: Extended XAdES signatures v1.1.1, (April 2016)*

XML Signature Syntax and Processing[2], W3C Recommendation, 11 April 2013

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 https://www.iso.org/obp

— IEC Electropedia: available at http://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

3.2
profile

[1] Available from https://www.etsi.org/standards-search.
[2] Available from https://www.w3.org/TR/xmldsig-core/.

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

3.3
XML signature
XmlDsig
signature syntax and processing for a given message

Note 1 to entry: Defined in XML Signature Syntax and Processing, W3C Recommendation 11 April 2013.

3.4
XAdES digital signature
XAdES
XML based digital signature defined in ETSI EN 319 132-2 for which the signer can be identified and any illegal data alteration detected

Note 1 to entry: Digital signatures specified in ETSI documents aim at supporting electronic signatures and electronic seals

3.5
XAdES with time
XAdES-T
generic term for the incorporation of all the XAdES digital signature defined in ETSI EN 319 132-2 with information to ascertain SigningTime, and intermediate form for *long term signature* (3.1) *profile* (3.2)

3.6
XAdES with validation data
XAdES-X-Long
generic term for the incorporation of all the material required for validating the signature, and intermediate form for *long term signature* (3.1) *profile* (3.2)

3.7
archival XAdES
XAdES-A
generic term for the incorporation of electronic time stamps that allow validation of the digital signature long time after its generation, and *long term signature* (3.1) *profile* (3.2)

4 Long term signature profiles

4.1 Defined profile

4.1.1 General

In order to make digital signatures verifiable for a 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 ensured. To meet these requirements, this document defines a long term profile for XAdES and forms to construct signature data conforming to the profile:

a) XAdES-T profile (intermediate form): signature with signature timestamp

b) XAdES-X-Long form (intermediate form): form added validation information to a)

c) XAdES-A profile: form timestamped or protected for long term availability, which is extended from b)

Table 1 lists the correspondence between of various profiles. See Annex C "(informative) Differences of required level between European EN and ISO specification" for differences European EN and ISO profiles at each level.

Table 1 — Signature genarate profiles

14533–2:— XAdES ISO profile	14533–2:2012 XAdES ISO profiles	ETSI EN 319 132–2 Extended signatures
--	--	XAdES-E-BES/EPES
XAdES-T profile	XAdES-T profile	XAdES-E-T
(XAdES-X-Long form)	--	XAdES-E-X-Long
XAdES-A profile	XAdES-A profile	XAdES-E-A

4.1.2 Supplier's declaration of conformance

If first-party conformity assessment is used, the implementer shall make a declaration of conformity to this part of ISO 14533 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 See ISO/IEC 17050-1:2004, Conformity assessment - Supplier's declaration of conformity - Part 1: General requirements

4.1.3 XML namespaces

This document uses the URI namespaces and prefixes listed below:

- http://www.w3.org/2000/09/xmldsig# (prefix: ds)
- http://uri.etsi.org/01903/v1.3.2# (prefix: xs)
- http://uri.etsi.org/01903/v1.4.1# (prefix: xs141)

4.1.4 Operation of long term signature

Figure 1 shows operation of standard long term signature procedure.

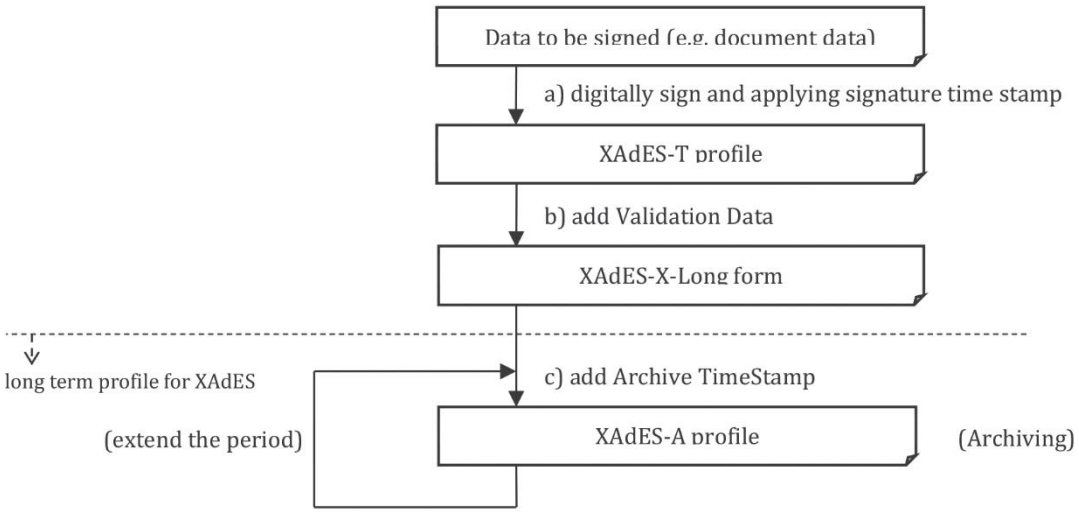

Figure 1 — Operation of long term signature

Figure 2 shows timing of standard long term signature procedure.

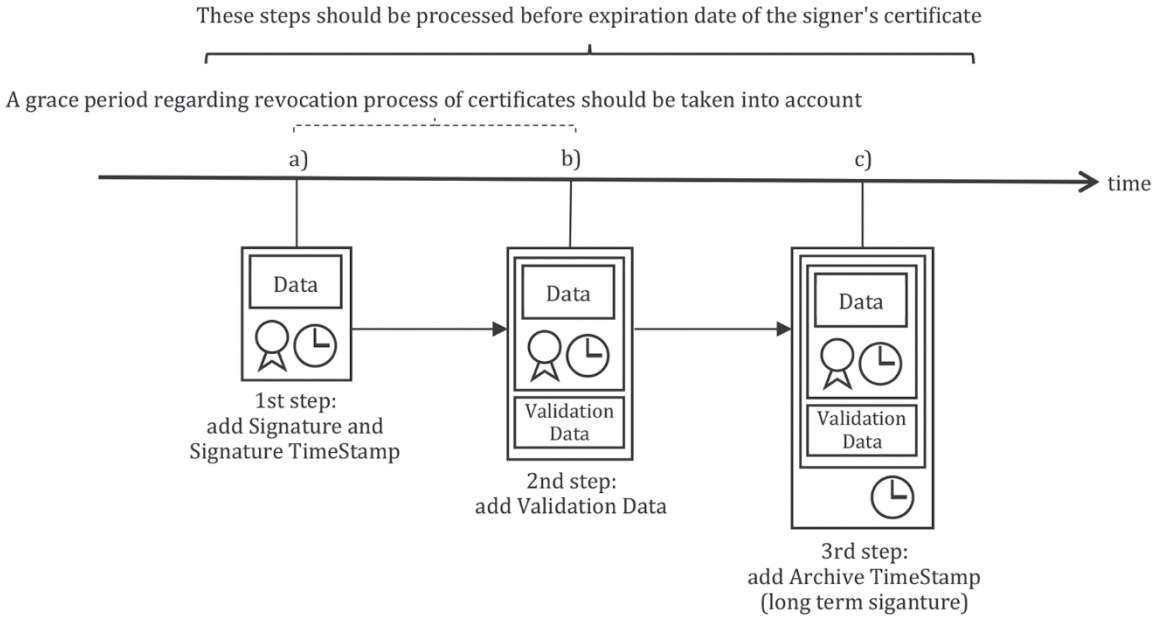

Figure 2 — Timing of long term signature step

4.2 Representation of the required level

This document defines the following representation methods for the required level (as form and profile) of each element constituting XAdES-T profile data, XAdES-X-Long form data and XAdES-A profile data.

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

4.3 Standard for setting the required level

The required level of each element constituting XAdES-T profile data, XAdES-X-Long form data and XAdES-A profile 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 XAdES, and those necessary for the generation and validation of long term signatures. The elements whose required level is “Optional” in the definition of XAdES 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 DataObjectFormat

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

EXAMPLE 3 Attribute certificate, Time mark

NOTE The archiving-type time stamp 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.

4.4 Action to take when an optional element is not implemented

The following actions shall be taken when the XAdES data used in a validation transaction contains an unimplemented element.

a) When the required level of a parent element is "Mandatory" and one or more subelements shall be selected, or one or more relevant optional elements shall be selected, the validator shall be cautioned that validation requires implementation of element(s); otherwise, validation cannot be performed.

EXAMPLE In a validation transaction, a OCSPValue element is detected where only the processing of CRLValue elements, among all other optional elements in RevocationValues, is implemented.

b) When xs:CounterSignature (see 4.5.4) is an unimplemented element, the validator shall be cautioned that validation requires implementation of said element; otherwise, validation cannot be performed.

c) Optional elements other than those specified above may be ignored for implementation.

4.5 XAdES-T profile

4.5.1 General

4.5.2, 4.5.3 and 4.5.4 specify the required levels of constituent elements of XAdES-T profile data.

4.5.2 Signature element

Table 2 specifies the required level of each constituent element of XML signature. The required level shall be “Conditional” for any elements not listed in Table 2.

Table 2 — Signature element

Element or attribute	Required level	XMLDSig reference
Id attribute	**M**[a]	**4.2**
ds:SignedInfo	**M**	**4.4**
ds:CanonicalizationMethod	**M**	**4.4.1**
ds:SignatureMethod	**M**	**4.4.2**
ds:Reference	**M**	**4.4.3**
ds:Transforms	**O**	**4.4.3.4**
ds:DigestMethod	**M**	**4.4.3.5**
ds:DigestValue	**M**	**4.4.3.6**
ds:SignatureValue	**M**	**4.3**
ds:KeyInfo	**O**[b]	**4.5**

ds:Object	**M**	**4.6**

[a] "Optional" in an XML signature, but "Mandatory" in ETSI EN 319 132.

[b] If the xs:SigningCertificateV2 qualifying property (Table 3) is incorporated to the signature, no restrictions apply to ds:KeyInfo element. Otherwise, then the following restrictions apply:

— the ds:KeyInfo element shall include a ds:X509Data containing the signing certificate;

— the ds:KeyInfo element may also contain other certificates;

— the ds:SignedInfo element shall contain a ds:Reference element that refers to ds:KeyInfo;

4.5.3 Object element, SignedSignatureProperties element

Table 3 specify the required levels of elements that constitute signed properties. The required level shall be "Conditional" for any signed and unsigned property elements not listed in Table 3.

Table 3 — Object element, SignedSignatureProperties element

Element	Required level	ETSI EN 319 132–1 v1.1.1 reference
xs:QualifyingProperties	**M**[a]	**4.3**
xs:SignedProperties	**M**	**4.3.2**
xs:SignedSignatureProperties	**M**	**4.3.4**
xs:SigningTime	**O**[b]	**5.2.1**
xs:SigningCertificateV2	**O**[b,c]	**5.2.2**
xs:SigningCertificate	**C**[d]	–-
xs:SignaturePolicyIdentifier	**C**	**5.2.9**
xs:SignatureProductionPlaceV2	**C**	**5.2.5**
xs:SignatureProductionPlace	**C**[d]	–-
xs:SignerRoleV2	**C**	**5.2.6**
xs:SignerRole	**C**[d]	–-
xs:SignedDataObjectProperties	**C**	**4.3.5**
xs:DataObjectFormat	**C**[b]	**5.2.4**
xs:Description	**C**	**5.2.4**
xs:ObjectIdentifier	**C**	**5.2.4**
xs:MimeType	**C**[b]	**5.2.4**
xs:Encoding	**C**	**5.2.4**
xs:CommitmentTypeIndication	**C**	**5.2.3**
xs:AllDataObjectsTimeStamp	**C**	**5.2.8.1**
xs:IndividualDataObjectsTimeStamp	**C**	**5.2.8.2**

[a] The Id attribute value of the signature element shall be entered in the target attribute.

[b] Mandatory in ETSI EN 316 132-1 v1.1.1 Baseline Signature.

[c] Either xs:SigningCerticicateV2 or ds:KeyInfo (Table 2) is required.

[d] These elements are used for past compatibility and reference to ETSI TS 101 903 v1.1.1.

4.5.4 Object element, UnsignedSignatureProperties element

Table 4 specify the required levels of elements that constitute unsigned properties. The required level shall be "Conditional" for any signed and unsigned property elements not listed in Table 4.

Table 4 — Object element, UnsignedSignatureProperties element

Element	Required level	ETSI EN 319 132–1 v1.1.1 reference
xs:QualifyingProperties	**M**	**4.3**
xs:UnsignedProperties	**M**	**4.3.2**
xs:UnsignedSignatureProperties	**M**	**4.3.6**
xs:CounterSignature	**O**	**5.2.7.2**
Trusted time	**M**	**5.3**
xs:SignatureTimeStamp	**O**[a]	**5.3**
other POE method	**C**	–-
xs:UnsignedDataObjectProperties	**C**	**4.3.7**

[a] Mandatory in ETSI EN 319 132-1 v1.1.1 Baseline Signature.

4.6 XAdES-X-Long form

4.6.1 General

4.6.2 and 4.6.3 specify the required levels of constituent elements of XAdES-X-Long data.

4.6.2 Structure of the XAdES-X-Long form

The XAdES-X-Long form is defined as an extended form of the XAdES-T profile to which the unsigned properties specified in Table 5 are added. The required level of each element of the portion corresponding to XAdES-T shall be as specified in 4.5.

4.6.3 Additional UnsignedSignatureProperties element

The required level of each element added to unsigned properties shall be as stated in Table 5. The required level shall be "Conditional" for any element not specified in Table 5.

NOTE Unsigned property elements not listed in Table 4, 5 and 6 include, but are not limited to, CompleteCertificateRefs and CompleteRevocationRefs set forth in Table 5. XAdES-T and XAdES-X-Long data to which CompleteCertificateRefs and CompleteRevocationRefs are added can be made compliant with the XAdES-T profile and XAdES-X-Long form by providing these elements separately for the processing of these elements.

Table 5 — Additional UnsignedSignatureProperties for XadES-X-Long form

Element or processing method	Required level	ETSI EN 319 132–1 v1.1.1 reference
xs141:TimeStampValidationData	**C**	**5.5.1**
xs:CertificateValues	**C**	**5.4.1**
xs:RevocationValues	**C**	**5.4.2**
xs141:CompleteCertificateRefsV2	**O**	**A.1.1**
xs:CompleteCertificateRefs	**C**[a]	–-
xs:CompleteRevocationRefs	**C**[a]	**A.1.2**
xs:CRLRef	**O**	**A.1.2**
xs:OCSPRef	**O**	**A.1.2**

xs:OtherRef	**C**	**A.1.2**
xs141:AttributeCetrificateRefsV2	**C**	**A.1.3**
xs:AttributeCetrificateRefs	**C**[c]	**--**
xs:AttributeRevocationRefs	**C**[c]	**A.1.4**
xs141:SigAndRefsTimeStampV2	**C**	**A.1.5.1**
not distributed case	**M**	**A.1.5.1.2**
distributed case	**C**	**A.1.5.1.3**
xs:SigAndRefsTimeStamp	**C**[a]	**--**
xs141:RefsOnlyTimeStampV2	**C**	**A.1.5.2**
not distributed case	**M**	**A.1.5.2.2**
distributed case	**C**	**A.1.5.2.3**
xs:RefsOnlyTimeStamp	**C**	**--**
xs:CertificateValues	**M**	**5.4.1**
xs:EncapsulatedX509Certificate	**O**	**5.4.1**
xs:OtherCertificate	**C**	**5.4.1**
Certificates maintained by trusted service	**C**[b]	**--**
xs:RevocationValues	**M**	**5.4.2**
xs:CRLValues	**O**	**5.4.2**
xs:OCSPValues	**O**	**5.4.2**
xs:OtherValues	**C**	**5.4.2**
Certificates maintained by trusted service	**C**[b]	**--**
xs:AttrAuthoritiesCertValues	**C**[c]	**5.4.3**
xs:AttributeRevocationValues	**C**[c]	**5.4.4**
Any unsigned signature property defined in any other version of XAdES	**C**	**--**

[a] These elements are used for past compatibility and reference to ETSI TS 101 903 v1.1.1. These elements are obsolete and should not be used to create new signatures and should be used only for verification.

[b] If a certification authority (CA) or other trusted service is trusted to maintain certificates for the archiving period there is no need to hold them with the signature.

[c] AttrAuthoritiesCertValues and AttributeRevocationValues, and not distributed cases and distributes cases are not defined in ETSI TS 101 903 v1.1.1 and 1.2.1. AttributeCetrificateRefs and AttributeRevocationRefs are also not defined in v1.1.1.

4.7 XAdES-A profile

4.7.1 General

4.7.2 and 4.7.3 specify the required levels of constituent elements of XAdES-A data.

4.7.2 Structure of the XAdES-A profile

The XAdES-A profile is defined as an extended form of the XAdES-X-Long form to which the unsigned properties specified in Table 6 are added. The required level of each element of the portion corresponding to XAdES-X-Long shall be as specified in 4.6.

4.7.3 Additional UnsignedSignatureProperties element for XAdES-A profile

The required level of each element added to unsigned properties shall be as stated in Table 6. The required level shall be “Conditional” for any element not specified in Table 6.

Table 6 — Additional UnsignedSignatureProperties

Element or processing method	Required level	ETSI EN 319 132–1 v1.1.1 reference
Archiving	**M**[a]	**--**
xs141:ArchiveTimeStamp	**O**	**5.5.2**
not distributed case	**M**	**5.5.2.2**
distributed case	**C**	**5.5.2.3**
Evidence Record	**C**[b]	**--**
xs:ArchiveTimeStamp	**C**[c]	**--**
Other method	**C**[a]	**--**
xs141:TimeStampValidationData	**C**[d]	**5.5.1**
xs:CertificateValues	**C**	**5.4.1**
xs:RevocationValues	**C**	**5.4.2**
xs141:RenewedDigests	**C**[e]	**5.5.3**
Any unsigned signature property defined in any other version of XAdES	**C**	**--**

[a] If the other trusted service alternative to "ArchiveTimeStamp" is trusted to maintain time stamping for the archiving period "other method" can be applied.

[b] Defined in IETF RFC 6283.

[c] This element is used for past compatibility and reference to ETSI TS 101 903 v1.1.1. This element is obsolete and should not be used to create new signatures and should be used only for verification.

[d] See 4.8.

[e] for Manifest element.

4.8 Time stamp validation data

The validation of past time stamps requires certificates and revocation information up to the trust anchor. Time stamp validation data requires certificates in the certification path from TSA (time stamping authority) certificates to trust anchor certificates, and the revocation information pertaining to each such certificate. See Annex B "(normative) Structure of time-stamp token" for additional information.

Validation data may be stored with XAdES-A data as described below. When not stored with XAdES-A data, validation data shall be stored by another secure means including, but not limited to, storage by CA as a TTP (trusted third party) or by TSA.

In past time stamp validation, validation data stored as described below or by another secure means may also be used.

a) Validation data for signature timestamp shall be stored upon generation at one of the places set forth below or by CA, etc.

    1) The following element within unsigned properties:

        — xs141:TimeStampValidationData (see 4.6.3)

    2) The following elements within unsigned properties:

        — xs:CertificateValues (see 4.6.3)

— xs:RevocationValues (see 4.6.3)

3) The following elements within the timestamp token in the signature timestamp (signature timestamp token):

— CertificateSet (see B.3)

— RevocationInfoChoices (see B.3)

4) The following elements within the unsigned attributes of the signature timestamp token:

— CertificateValues (see B.3)

— RevocationValues (see B.3)

b) Validation data for archive timestamp shall be stored upon generation at one of the places set forth below or by CA, etc.

1) The following element within unsigned properties:

— xs141:TimeStampValidationData (see 4.6.3)

2) The following elements within the timestamp token in the archive timestamp (archive timestamp token):

— CertificateSet (see B.3)

— RevocationInfoChoices (see B.3)

3) The following elements within the unsigned attributes of the archive timestamp token:

— CertificateValues (see B.3)

— RevocationValues (see B.3)

Annex A
(normative)

Supplier's declaration of conformity and its attachment

A.1 General

This annex sets forth the form of the supplier's declaration of conformity to the XAdES 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

No. _____

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.

XAdES-T profile and/or XAdES-A profile

The implemented elements are as specified in A.2 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.3.8.

NOTE Check the implemented elements shown in the creator and validator columns of Tables A.1 to A.8.

A.3.2 Version number of ETSI EN 319 132-2 to be referenced

A.3.3 Scope of profile implementation

Table A.1 — Profile implementation

Profile identifier	Creator	Validator
XAdES-T		
XAdES-A		

A.3.4 Conformity to the XAdES-T profile

Table A.2 — Signature element

Element	Required level	Creator	Validator
Id attribute	M[a]		
ds:SignedInfo	M		
ds:CanonicalizationMethod	M		
ds:SignatureMethod	M		
ds:Reference	M		
ds:Transforms	O		
ds:DigestMethod	M		
ds:DigestValue	M		
ds:SignatureValue	M		
ds:KeyInfo	O[b]		
ds:Object	M		

[a] "Optional" in an XML signature, but "Mandatory" in ETSI EN 319 132.

[b] If the xs:SigningCertificateV2 qualifying property (Table 3) is incorporated to the signature, no restrictions apply to ds:KeyInfo element. Otherwise, then the following restrictions apply:

— the ds:KeyInfo element shall include a ds:X509Data containing the signing certificate;

— the ds:KeyInfo element may also contain other certificates;

— the ds:SignedInfo element shall contain a ds:Reference element that ensures that the signing.

Table A.3 — Object element

Element	Required level	Creator	Validator
xs:QualifyingProperties	M		
xs:SignedProperties	M		
xs:UnsignedProperties	O		
xs:QualifyingPropertiesReference	C		

Table A.4 — Singed Properties element

Element	Required level	Creator	Validator
xs:SignedSignatureProperties	M		
xs:SigningTime	O[a]		

xs:SigningCertificateV2	**O**[a,b]		
xs:SigningCertificate	**C**[c]		
xs:SignaturePolicyIdentifier	**C**		
xs:SignatureProductionPlaceV2	**C**		
xs:SignatureProductionPlace	**C**[c]		
xs:SignerRoleV2	**C**		
xs:SignerRole	**C**[c]		
xs:SignedDataObjectProperties	**C**		
xs:DataObjectFormat	**C**[a]		
xs:Description	**C**		
xs:ObjectIdentifier	**C**		
xs:MimeType	**C**[a]		
xs:Encoding	**C**		
xs:CommitmentTypeIndication	**C**		
xs:AllDataObjectsTimeStamp	**C**		
xs:IndividualDataObjectsTimeStamp	**C**		

[a] Mandatory in ETSI EN 319 132–1 v1.1.1 Baseline Signature.

[b] Either xs:SigningCertificateV2 or ds:KeyInfo (Table 2) is required.

[c] These elements are used for past compatibility and reference to ETSI TS 101 903 v1.1.1.

Table A.5 — Unsigned properties

Element	Required level	Creator	Validator
xs:UnsignedSignatureProperties	**M**		
xs:CounterSignature	**O**		
Trusted time	**M**		
xs:SignatureTimeStamp	**O**[a]		
xs:Time mark or other method	**C**		
xs:UnsignedDataObjectProperties	**C**		

[a] Mandatory in ETSI EN 319 132–1 v1.1.1 Baseline Signature.

A.3.5 Conformity to the XAdES-X-Long form

Table A.6 — Additional Unsigned properties

Element	Required level	Creator	Validator
xs141:TimeStampValidationData	**C**		
xs:CertificateValues	**C**		
xs:RevocationValues	**C**		
xs141:CompleteCertificateRefsV2	**O**		
xs:CompleteCertificateRefs	**C**[a]		
xs:CompleteRevocationRefs	**C**[a]		
xs:CRLRef	**O**		

xs:OCSPRef	**O**		
xs:OtherRef	**C**		
xs141:AttributeCetrificateRefsV2	**O**		
xs:AttributeCetrificateRefs	**C**[c]		
xs:AttributeRevocationRefs	**C**[c]		
xs141:SigAndRefsTimeStampV2	**C**		
not distributed case	**M**		
distributed case	**C**		
xs:SigAndRefsTimeStamp	**C**[a]		
xs141:RefsOnlyTimeStampV2	**C**		
not distributed case	**M**		
distributed case	**C**		
xs:RefsOnlyTimeStamp	**C**		
xs:CertificateValues	**M**		
xs:EncapsulatedX509Certificate	**O**		
xs:OtherCertificate	**C**		
Certificates maintained by trusted service	**C**[b]		
xs:RevocationValues	**M**		
xs:CRLValues	**O**		
xs:OCSPValues	**O**		
xs:OtherValues	**C**		
Certificates maintained by trusted service	**C**[b]		
xs:AttrAuthoritiesCertValues	**C**[c]		
xs:AttributeRevocationValues	**C**[c]		
Any unsigned signature property defined in any other version of XAdES	**C**		

[a] These elements are used for past compatibility and reference to ETSI TS 101 903 v1.1.1. These elements are obsolete and should not be used to create new signatures and should be used only for verification.

[b] If a certification authority (CA) or other trusted service is trusted to maintain certificates for the archiving period there is no need to hold them with the signature.

[c] AttrAuthoritiesCertValues and AttributeRevocationValues, and not distributed cases and distributes cases are not defined in ETSI TS 101 903 v1.1.1 and 1.2.1. AttributeCetrificateRefs and AttributeRevocationRefs are also not defined in v1.1.1.

A.3.6 Conformity to the XAdES-A profile

Table A.7 — Additional Unsigned properties

Element	Required level	Creator	Validator
Archiving	**M**[a]		
xs141:ArchiveTimeStamp	**O**		
not distributed case	**M**		
distributed case	**C**		
Evidence Record	**C**[b]		

xs:ArchiveTimeStamp	**C**[c]		
Other method	**C**[a]		
xs141:TimeStampValidationData	**C**[d]		
xs:CertificateValues	**C**		
xs:RevocationValues	**C**		
xs141:RenewedDigests	**C**[e]		
Any unsigned signature property defined in any other version of XAdES	**C**		

[a] If the other trusted service alternative to "ArchiveTimeStamp" is trusted to maintain time stamping for the archiving period "other method" can be applied.

[b] Defined in IETF RFC 6283.

[c] This element is used for past compatibility and reference to ETSI TS 101 903 v1.1.1. This element is obsolete and should not be used to create new signatures and should be used only for verification.

[d] See 4.8.

[e] For Manifest element.

A.3.7 Specifications to be referenced by elements "Conditional"

Table A.8 — "Conditional" elements

No.	Element name	Referenced specification
1		
2		

NOTE Tables A.2 to A.7, give the names of elements identified as "Conditional" and the referenced specifications.

A.3.8 Remarks

Annex B
(normative)

Structure of time-stamp token

B.1 General

This annex sets forth the requirements for the structure of a timestamp token in a long term signature.

B.2 Normative specifications

The signature timestamp token and archive timestamp token in this document shall conform to CMS (RFC 5652), TSP (RFC 3161), CAdES (ISO 14533-1).

B.3 Required level of constituent elements

The required level of each element of the signature timestamp token and archive timestamp token shall be as specified in Table B.1.

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

Element	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	**O**	
AttributeCertificateV1	**O**	
AttributeCertificateV2	**O**	
OtherCertificateFormat	**O**	
RevocationInfoChoices (crls)	**O**	
CertificateList	**O**	
OtherRevocationInfoFormat	**O**	
SignerInfos	**M**	
SignerInfo	**M**	
CMSVersion	**M**	
SignerIdentifier	**M**	
IssuerAndSerialNumber	**O**	
SubjectKeyIdentifier	**O**	

igestAlgorithmIdentifier	**M**	
SignedAttributes	**M**	
ContentType	**M**	**id-ct-TSTInfo**
MessageDigest	**M**	
SigningCertificateReference	**M**	
ESS SigningCertificate	**O**	
ESS SigningCertificate v2	**O**	
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**	

Annex C
(informative)

Differences of required level between European EN and ISO specification

"ETSI EN 319 132-1 XAdES digital signatures Part 1" and "ISO/DIS 14533-2:2020" have different required levels. See Tables C.1 to C.4.

Table C.1 — Signature element

Element	ISO 14533-2 Required level	ETSI EN 319 132–1 v1.1.1 Required level
ds:KeyInfo/ds:X509Data	O	shall be present

Table C.2 — Object element, SignedSignatureProperties element

Element	ISO 14533-2 Required level	ETSI EN 319 132–1 v1.1.1 Required level
xs:SigningTime	O	shall be present
xs:SigningCertificateV2	O	shall be present
xs:DataObjectFormat/xs:MimeType	C	shall be present

Table C.3 — Object element, UnsignedSignatureProperties element

Element	ISO 14533-2 Required level	ETSI EN 319 132–1 v1.1.1 Required level
xs:SignatureTimeStamp	O	shall be present

Table C.4 — Additional UnsignedSignatureProperties

Element or *Processing method*	ISO 14533-2 Required level	ETSI EN 319 132–1 v1.1.1 Required level
xs141:ArchiveTimeStamp	O	shall be present
xs:ArchiveTimeStamp	C	shall not be present

Bibliography

[1] ETSI TS 101 903 XML Advanced Electronic Signatures (XAdES) v1.4.1, (2009-06), Available from <https://www.etsi.org/standards-search>

[2] ETSI EN 319 132-1, XAdES digital signatures Part 1: Building blocks and XAdES baseline signatures v1.1.1, (April 2016), Available from <https://www.etsi.org/standards-search>

[3] IETF RFC 5652, Cryptographic Message Syntax (CMS), Available from <https://www.ietf.org/>

[4] ISO/IEC 18014-2:2009 Information technology – Security techniques – Time-stamping services – Part 2: Mechanisms producing independent tokens

[5] IETF RFC 3161, Time-Stamp Protocol (TSP), Available from <https://www.ietf.org/>

[6] IETF RFC 6283, Extensible Markup Language Evidence Record Syntax (XMLERS), Available from <https://www.ietf.org/>