INTERNATIONAL STANDARD

ISO 14533-2

First edition
2012-09-15

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

Part 2: Long term signature profiles for XML Advanced Electronic Signatures (XAdES)

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

Partie 2: Profils de signature à long terme pour les signatures électroniques avancées XML (XAdES)

Reference number
ISO 14533-2:2012(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web 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 **Symbols** ... 2

5 **Requirements** ... 2

6 **Long term signature profiles** ... 2
6.1 **Defined profiles** ... 2
6.2 **Representation of the required level** ... 3
6.3 **Standard for setting the required level** ... 3
6.4 **Action to take when an optional element is not implemented** ... 4
6.5 **XAdES-T profile** ... 4
6.6 **XAdES-A profile** ... 6
6.7 **Timestamp validation data** ... 8

Annex A (normative) **Supplier's declaration of conformity and its attachment** ... 9

Annex B (normative) **Structure of timestamp token** ... 14

Bibliography ... 16

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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

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.

ISO 14533-2 was prepared by Technical Committee ISO/TC 154, *Processes, data elements and documents in commerce, industry and administration*.

ISO 14533 consists of the following parts, under the general title *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)*

— *Part 2: Long term signature profiles for XML Advanced Electronic Signatures (XAdES)*

Introduction

The purpose of this part of ISO 14533 is to ensure the interoperability of implementations with respect to long term signatures that make electronic signatures verifiable for a long term. Long term signature specifications referenced by each implementation cover XML Advanced Electronic Signatures (XAdES) developed by the European Telecommunications Standards Institute (ETSI).

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

Part 2: Long term signature profiles for XML Advanced Electronic Signatures (XAdES)

1 Scope

This part of ISO 14533 specifies the elements, among those defined in XML Advanced Electronic Signatures (XAdES), 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 has already existed.

NOTE XML Advanced Electronic Signatures (XAdES) is the extended specification of XML-Signature Syntax and Processing, used widely.

2 Normative references

The following referenced documents are indispensable for the application 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 TS 101 903 v1.4.1 (2009-06), *XML Advanced Electronic Signatures (XAdES)* [1)]

3 Terms and definitions

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

3.1
XML signature
signature syntax and processing for a given message

NOTE XML signature is defined in *XML-Signature Syntax and Processing*, W3C Recommendation, 12 February 2002.

3.2
XML advanced electronic signature
XAdES
generic term for XML advanced electronic signatures defined in ETSI TS 101 903 for which the signer can be identified and any illegal data alteration detected

3.3
XAdES with time
XAdES-T
XML advanced electronic signature defined in ETSI TS 101 903 with information to ascertain SigningTime (e.g. signature timestamp)

1) Available from http://pda.etsi.org/pda/queryform.asp.

3.4
archival XAdES
XAdES-A
XML advanced electronic signature defined in ETSI TS 101 903 with information to enable the detection of any illegal alterations of information pertaining to the signature, including the subject of the signature and validation data (e.g. archive timestamp)

3.5
signature element
element that serves as a route for the XML signature. There may be two or more signature elements for one subject of a signature

4 Symbols

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

— C Conditional

— M Mandatory

— O Optional

5 Requirements

5.1 The generation or validation of XAdES-T data conforms to this part of ISO 14533 provided that the following requirements are met:

a) all processing of elements whose required level is “Mandatory” in the XAdES-T profile, as specified in this part of ISO 14533, shall be included;

b) detailed specifications pertaining to the processing of any element whose required level is “Conditional” in the XAdES-T profile, as specified in this part of ISO 14533, shall be provided.

5.2 The generation or validation of XAdES-A data conforms to this part of ISO 14533 provided that the following requirements are met:

a) all processing of elements whose required level is “Mandatory” in the XAdES-A profile, as specified in this part of ISO 14533, shall be included;

b) detailed specifications pertaining to the processing of any element whose required level is “Conditional” in the XAdES-A profile, as specified in this part of ISO 14533, shall be provided.

5.3 When 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 Figure 1 shows the positioning of the generation and validation of XAdES-T data and XAdES-A data.

6 Long term signature profiles

6.1 Defined profiles

In order to make electronic 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 part of ISO 14533 defines the following two profiles with respect to XAdES:

a) XAdES-T profile: a profile pertaining to the generation and validation of XAdES-T data;

b) XAdES-A profile: a profile pertaining to the generation and validation of XAdES-A data.

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

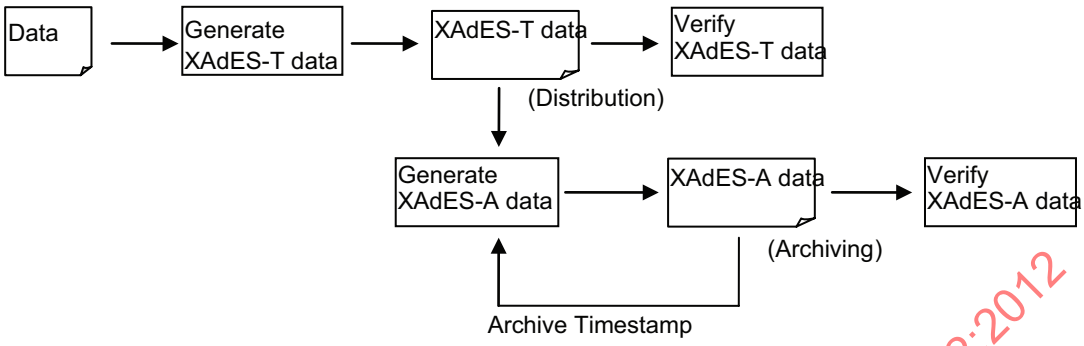

Figure 1 — Relation between XAdES-T data and XAdES-A data

6.2 Representation of the required level

This part of ISO 14533 defines the following representation methods for the required level (as a profile) of each element constituting XAdES-T data and XAdES-A 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.

6.3 Standard for setting the required level

The required level of each element constituting XAdES-T data and XAdES-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 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 OtherCertificateFormat.

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

EXAMPLE DataObjectFormat.

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

EXAMPLES 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 Action to take when an optional element is not implemented

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

a) When the required level of an upper-level element is mandatory and one or more subordinate optional elements shall be selected, or one or more relevant optional elements shall be selected, the validator shall be cautioned that validation requires implementation of said element(s); otherwise, validation cannot be performed.

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

b) When CounterSignature 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.

6.5 XAdES-T profile

6.5.1 General

The required levels of constituent elements of XAdES-T data are specified in 6.5.2 and 6.5.3.

6.5.2 Signature element

Table 1 specifies the required level of each constituent element of XML signature. The required level shall be "Conditional" for any elements not listed in Table 1.

Table 1 — Signature element

Element or attribute [a]	Required level	ETSI TS 101 903 v1.4.1 Reference
Id attribute	M [b]	4.4
ds:SignedInfo	M	4.4
ds:CanonicalizationMethod	M	4.4
ds:SignatureMethod	M	4.4
ds:Reference	M	4.4
ds:Transforms	O	4.4
ds:DigestMethod	M	4.4
ds:DigestValue	M	4.4
ds:SignatureValue	M	4.4
ds:KeyInfo	O [c]	4.4
ds:Object	M	4.4

[a] The prefix "ds" corresponds to the XML signature namespace.

[b] "Optional" in an XML signature, but "Mandatory" in ETSI TS 101 903.

[c] Either ds:KeyInfo or SigningCertificate (Table 3) is required. If ds:KeyInfo is selected (Mandatory in ETSI TS 101 903 v1.1.1), an X.509 data element defined in the XML signature shall be included as a subelement.

6.5.3 Object element, SignedProperties element, UnsignedProperties element

Tables 2, 3 and 4 specify the required levels of elements that constitute signed properties and unsigned properties. The required level shall be “Conditional” for any signed and unsigned property elements not listed in Tables 2, 3 and 4.

NOTE Unsigned property elements not listed in Tables 2, 3 and 4 include, but are not limited to, CompleteCertificateReferences and CompleteRevocationReferences set forth in Table 5. XAdES-T data to which CompleteCertificateReferences and CompleteRevocationReferences are added can be made compliant with the XAdES-T profile by separately providing for the processing of these elements.

Table 2 — Object element

Element	Required level	Condition	ETSI TS 101 903 v1.4.1 Reference
QualifyingProperties	M	The Id attribute value of the signature element shall be entered in the target attribute.	6.2
SignedProperties	M		6.2.1
UnsignedProperties	O		6.2.2
QualifyingPropertiesReference	C		6.3.2

Table 3 — SignedProperties element

Element	Required level	ETSI TS 101 903 v1.4.1 Reference
SignedSignatureProperties	M	6.2.3
SigningTime	O [a]	7.2.1
SigningCertificate	O [a,b]	7.2.2
SignaturePolicyIdentifier	C	7.2.3
SignatureProductionPlace	C	7.2.7
SignerRole	C	7.2.8
SignedDataObjectProperties	C	6.2.4
DataObjectFormat	C	7.2.5
CommitmentTypeIndication	C	7.2.6
AllDataObjectsTimeStamp	C	7.2.9
IndividualDataObjectsTimeStamp	C	7.2.10

[a] Mandatory in ETSI TS 101 903 v1.1.1.

[b] Either SigningCertificate or ds:KeyInfo (Table 1) is required.

Table 4 — UnsignedProperties element

Element	Required level	ETSI TS 101 903 v1.4.1 Reference
UnsignedSignatureProperties	M	6.2.5
CounterSignature	O	7.2.4
Trusted time	M	7.3
SignatureTimeStamp	O	7.3
Time mark or other method	C	7.3
UnsignedDataObjectProperties	C	6.2.6

6.6 XAdES-A profile

6.6.1 General

The required levels of constituent elements of XAdES-T data are specified in 6.6.2 and 6.6.3.

6.6.2 Structure of the XAdES-A profile

The XAdES-A profile 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 6.5.

6.6.3 Additional UnsignedSignatureProperties

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.

Table 5 — Additional UnsignedSignatureProperties

Element or Processing method	Required level	ETSI TS 101 903 v1.4.1 Reference
CompleteCertificateRefs	O [a]	7.4.1
CompleteRevocationRefs	O [a]	7.4.2
CRLRef	O	7.4.2
OCSPRef	O	7.4.2
OtherRef	C	7.4.2
AttributeCetrificateRefs	C	7.4.3
AttributeRevocationRefs	C	7.4.4
SigAndRefsTimeStamp	C [b]	7.5.1
not distributed case	M	7.5.1.1
distributed case	C	7.5.1.2
RefsOnlyTimeStamp	C [b]	7.5.2
not distributed case	M	7.5.2.1
distributed case	C	7.5.2.2
CertificateValues	M	7.6.1
EncapsulatedX509Certificate	O	7.6.1
OtherCertificate	C	7.6.1
Certificates maintained by trusted service	C	[c]
RevocationValues	M	7.6.2
CRLValues	O	7.6.2
OCSPValues	O	7.6.2
OtherValues	C	7.6.2
Certificates maintained by trusted service	C	[c]
AttrAuthoritiesCertValues	C	7.6.3
AttributeRevocationValues	C	7.6.4
Archiving	M	[d]
ArchiveTimeStamp	O	8.2
not distributed case	M	8.2.1
distributed case	C	8.2.2
Evidence Record	C	[e]
Other method	C	[d]
Any unsigned signature property defined in any other version of XAdES	C	6.2.5

NOTE 1 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.

NOTE 2 ETSI TS 101 903 v1.3.2 defines different calculation mechanism, “not distributed case” or “distributed case”, depending on whether the timestamp property and timestamped properties have the same parent or not.

[a] Mandatory in ETSI TS 101 903 v1.1.1.

[b] Not recommended. If selected, either SigAndRefsTimeStamp or RefsOnlyTimeStamp may be selected. Either one is required under ETSI TS 101 903 v1.1.1.

[c] 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.

[d] If the other trusted service alternative to “ArchiveTimeStamp” is trusted to maintain timestamping for the archiving period “other method” can be applied.

[e] Defined in IETF RFC 4998.

6.7 Timestamp validation data

The validation of past timestamps requires certificates and revocation information up to the trust anchor. Timestamp validation data requires certificates in the certification path from TSA certificates to trust anchor certificates, and the revocation information pertaining to each such certificate.

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 or by TSA.

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

Annex B specifies the requirements relevant to the structure of a timestamp token.

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 elements within unsigned properties:

      — CertificateValues

      — RevocationValues

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

      — CertificateSet

      — RevocationInfoChoices

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

      — CertificateValues

      — RevocationValues

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

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

      — CertificateSet

      — RevocationInfoChoices

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

      — CertificateValues

      — RevocationValues

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.3.7.

NOTE Check the implemented elements shown in the generator and verifier columns of Tables A.1 to A.6.

A.3.2 Version number of ETSI TS 101 903 to be referenced

A.3.3 Scope of profile implementation

Table A.1 — Profile implementation

Profile identifier	Generator	Verifier
XAdES-T		
XAdES-A		

A.3.4 Conformity to the XAdES-T profile

Table A.2 — Signature element

Element	Required level	Generator	Verifier
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 TS 101 903.

[b] Either ds:KeyInfo or SigningCertificate (Table 3) is required. If ds:KeyInfo is selected (Mandatory in ETSI TS 101 903 v1.1.1), an X.509 data element defined in the XML signature shall be included as a subelement.

Table A.3 — Object element

Element	Required level	Generator	Verifier
QualifyingProperties	M		
SignedProperties	M		
UnsignedProperties	O		
QualifyingPropertiesReference	C		

Table A.4 — Singed properties element

Element	Required level	Generator	Verifier
SignedSignatureProperties	M		
SigningTime	O [a]		
SigningCertificate	O [a,b]		
SignaturePolicyIdentifier	C		
SignatureProductionPlace	C		
SignerRole	C		
SignedDataObjectProperties	C		
DataObjectFormat	C		
CommitmentTypeIndication	C		
AllDataObjectsTimeStamp	C		
IndividualDataObjectsTimeStamp	C		

[a] Mandatory in ETSI TS 101 903 v1.1.1.

[b] Either SigningCertificate or ds:KeyInfo (Table 1) is required.

Table A.5 — Unsigned properties

Element	Required level	Generator	Verifier
UnsignedSignatureProperties	M		
CounterSignature	O		
Trusted time	M		
SignatureTimeStamp	O		
Time mark or other method	C		
UnsignedDataObjectProperties	C		

A.3.5 Conformity to the XAdES-A profile

Table A.6 — Additional unsigned properties

Element	Required level	Generator	Verifier
CompleteCertificateRefs	O [a]		
CompleteRevocationRefs	O [a]		
CRLRef	O		
OCSPRef	O		
OtherRef	C		
AttributeCetrificateRefs	C		
AttributeRevocationRefs	C		
SigAndRefsTimeStamp	C [b]		
not distributed case	M		
distributed case	C		
RefsOnlyTimeStamp	C [b]		
not distributed case	M		
distributed case	C		
CertificateValues	M		
EncapsulatedX509Certificate	O		
OtherCertificate	C		
Certificates maintained by trusted service	C		
RevocationValues	M		
CRLValues	O		
OCSPValues	O		
OtherValues	C		
Certificates maintained by trusted service	C		
AttrAuthoritiesCertValues	C		
AttributeRevocationValues	C		
Archiving	M		
ArchiveTimeStamp	O		
not distributed case	M		
distributed case	C		
Evidence Record	C		
Other method	C		
Any unsigned signature property defined in any other version of XAdES	C		

NOTE 1 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.

NOTE 2 ETSI TS 101 903 v1.3.2 defines different calculation mechanism, “not distributed case” or “distributed case”, depending on whether the timestamp property and timestamped properties have the same parent or not.

[a] Mandatory in ETSI TS 101 903 v1.1.1.

[b] Not recommended. If selected, either SigAndRefsTimeStamp or RefsOnlyTimeStamp may be selected. Either one is required under ETSI TS 101 903 v1.1.1.

A.3.6 Specifications to be referenced by elements “Conditional”

No.	Element name	Referenced specification
1		
2		

NOTE Tables A.2 to A.6 give the names of elements identified as “Conditional” and the referenced specifications.

A.3.7 Remarks
