DRAFT INTERNATIONAL STANDARD

ISO/DIS 14533-2

ISO/TC **154**	Secretariat: **SAC**
Voting begins on: **2020-11-05**	Voting terminates on: **2021-01-28**

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

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

ICS: 35.240.63

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

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

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

This document is circulated as received from the committee secretariat.

Reference number
ISO/DIS 14533-2:2020(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

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 ISO/TC 154..

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:

— *Part 1: Profiles for CMS Advanced Electronic Signatures (CAdES)*

— *Part 2: Profiles for XML Advanced Electronic Signatures (XAdES)*

— *Part 3: Profiles for PDF Advanced Electronic Signatures (PAdES)*

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 standard 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 standard 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 standard avoids quoting and redefining those components defined in ETSI EN 319 132 specification.

In first edition (ISO 14533-2:2012), XAdES was an acronym for 'XML Advanced Electronic Signature'. In this second edition (ISO 14533-2:2020), 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.

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 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 has already existed.

This second edition cancels and replaces the first edition (ISO 14533-2:2012), first edition which updates its XAdES specification from ETSI v1.3.2 to v1.4.1. and updates to the referenced ETSI specification.

NOTE XAdES digital signatures 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.

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

ETSI EN 319-132-1, *XAdES digital signatures Part 1: Building blocks and XAdES baseline signatures v1.1.1, (April 2016)*

NOTE Available from https://www.etsi.org/standards-search.

ITU-T Recommendation X.509 (2005)/ *ISO/IEC 9594-8:2005, Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*

NOTE Available from https://www.itu.int/rec/T-REC-X.509-201610-I

3 Terms and definitions

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

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
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.

Note 2 to entry: Available from https://www.w3.org/TR/xmldsig-core/.

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

Note 2 to entry: In first edition (ISO 14533-2:2012), XAdES was an acronym for 'XML Advanced Electronic Signature'

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 profile

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 profile

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 profile

4 Long term signature profiles

4.1 Defined profile

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 part of ISO 14533 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 — Signature genarate profiles

14533–2:2020 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

4.1.1 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)

4.1.2 Operation of long term signature

Figure 1 shows operation of standard long term signature procedure.

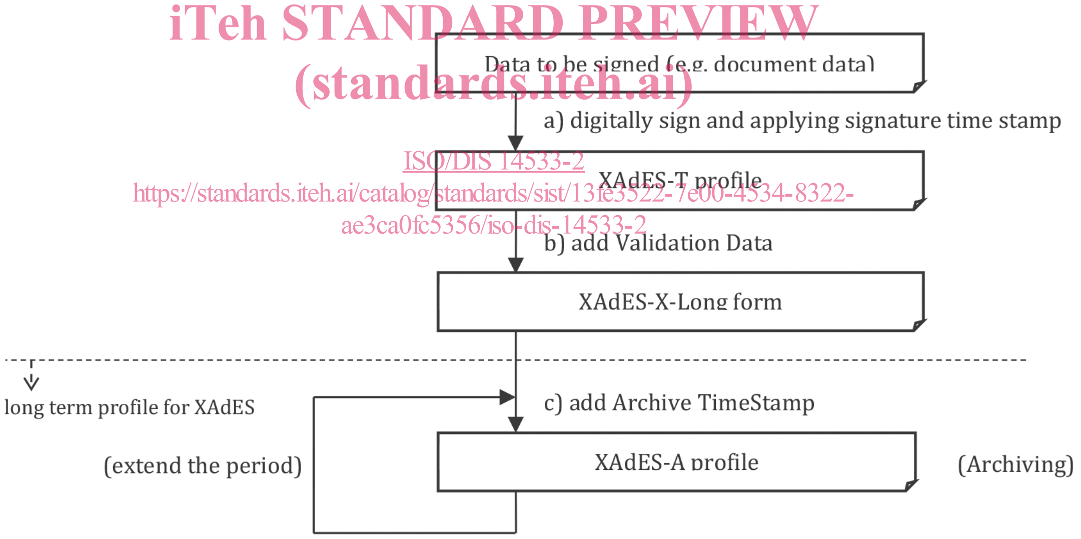

Figure 1 — Operation of long term signature

Figure 2 shows timing of standard long term signature procedure.

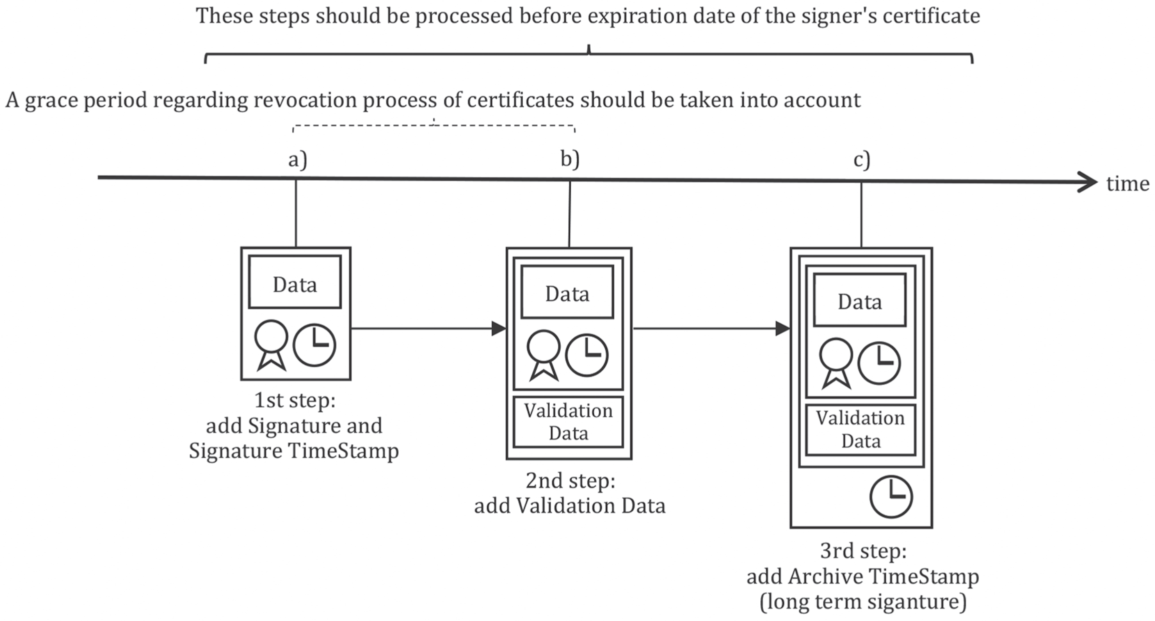

Figure 2 — Timing of long term signature step

4.2 Representation of the required level

This standard 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 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.

EXAMPLE 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 action 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 Clauses 4.5.3) 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

Subclauses 4.5.1 4.5.2 and 4.5.3 specify the required levels of constituent elements of XAdES-T profile data.

4.5.1 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*	Required level	XMLDSig Reference
Id attribute	**M** (NOTE 1)	**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**

NOTE 1 “Optional” in an XML signature, but “Mandatory” in ETSI EN 319 132.

NOTE 2 If the xs:SigningCertificateV2 qualifying property (Table 2) 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;