INTERNATIONAL STANDARD

ISO 14533-2

Second edition
2021-08

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

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

Reference number
ISO 14533-2:2021(E)

© ISO 2021



COPYRIGHT PROTECTED DOCUMENT

© ISO 2021

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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

Page

Foreword ... **iv**
Introduction ... **v**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms and definitions ... **1**
4 Long term signature profiles ... **2**
4.1 Defined profile ... 2
4.1.1 General ... 2
4.1.2 Supplier's declaration of conformance ... 3
4.1.3 XML namespaces ... 3
4.1.4 Operation of long term signature ... 3
4.2 Representation of the required level ... 4
4.3 Standard for setting the required level ... 4
4.4 Action to take when an optional element is not implemented ... 5
4.5 XAdES-T profile ... 5
4.5.1 General ... 5
4.5.2 Signature element ... 5
4.5.3 Object element, SignedSignatureProperties element ... 6
4.5.4 Object element, UnsignedSignatureProperties element ... 7
4.6 XAdES-X-Long form ... 7
4.6.1 General ... 7
4.6.2 Structure of the XAdES-X-Long form ... 7
4.6.3 Additional UnsignedSignatureProperties element ... 7
4.7 XAdES-A profile ... 8
4.7.1 General ... 8
4.7.2 Structure of the XAdES-A profile ... 9
4.7.3 Additional UnsignedSignatureProperties element for XAdES-A profile ... 9
4.8 Timestamp validation data ... 9
Annex A (normative) **Supplier's declaration of conformity and its attachment** ... **11**
Annex B (normative) **Structure of timestamp token** ... **16**
Annex C (informative) **Differences of required level between European EN and ISO specification** **18**
Bibliography ... **19**

© ISO 2021 – All rights reserved

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, *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 edition, XAdES becomes a proper noun and is used as ‘XAdES digital signature’;

— this edition supports XML namespace XAdES 1.4.1 elements;

— XAdES-A profile level is divided and explained as XAdES-X-Long form level;

— this edition describes the comparison with European EN in Annex C, "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.

© ISO 2021 – All rights reserved

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 it is still used in the document title.

© ISO 2021 – All rights reserved

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 widely-used extended specification of "XML-Signature Syntax and Processing".

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 terminology 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

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

2) Available from https://www.w3.org/TR/xmldsig-core/.

© ISO 2021 – All rights reserved

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: XML signature shall be as 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* (3.4) 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 timestamps 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).

© ISO 2021 – All rights reserved