Draft EN 319 132-2 V0.0.4 (2013-11)

XML Advanced Electronic Signaures (XAdES);

Part 2: XAdES Baseline Profile

STABLE DRAFT FOR PUBLIC REVIEW UNTIL 15 JANUARY 2014

Download the template for comments:

http://docbox.etsi.org/ESI/Open/Latest_Drafts/Template-for-comments.doc

Send comments to E-SIGNATURES_COMMENTS@LIST.ETSI.ORG

Reference
DEN/ESI-0019132-2

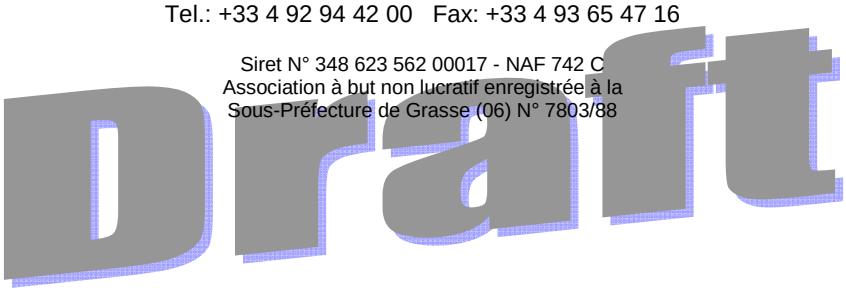
Keywords
<keywords>

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88



Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://ipr.etsi.org).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This draft European Standard (EN) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI).

The present document is part 2 of a multipart deliverable covering the specification of XML Advanced Electronic Signatures (XAdES). Full details of the entire series an be found in part 1 of ETSI EN 319 132 Part 1 [1].

Proposed national transposition dates	
Date of latest announcement of this EN (doa):	3 months after ETSI publication
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	6 months after doa
Date of withdrawal of any conflicting National Standard (dow):	6 months after doa

Introduction

This is part 2 of the multipart ETSI EN 319 132: “XML Advanced Electronic Signature (XAdES)”

EN 319 132-1 [1] (XAdES henceforth) specifies formats for Advanced Electronic Signatures built on XML SIG [2]. That part of the series defines a number of signed and unsigned optional signature properties, resulting in support for a number of variations in the signature contents and powerful processing requirements.

In order to maximise interoperability in communities applying XAdES to particular environments it is necessary to identify a common set of options that are appropriate to that environment. Such a selection is commonly called a profile.

The present document profiles EN 319 132-2 [1]] signatures contexts where AdES signatures are used and in particular its use in the context of the "Directive 2006/123/EC [i.1]] of the European Parliament and of the Council of 12 December 2006 on services in the internal market" (EU Services Directive henceforth).

EDITOR NOTE: a number of editor notes like this one appears througouht the document. These notes intend to attract readers’ attention and/or kindly request their feedback on certain specific issues.

1 Scope

The present document defines a baseline profile for XAdES that provides the basic features necessary for a wide range of business and governmental use cases for electronic procedures and communications to be applicable to a wide range of communities when there is a clear need for interoperability of AdES signatures used in electronic documents to be interchanged across borders. In particular it takes into account eSignature needs in the context of the EU Services Directive [i.1].

The profile defines four different conformance levels addressing incremental requirements to maintain the validity of the signatures over the long term, in a way that all the requirements addressed at a certain level are always addressed also by the levels above. Each level requires the presence of certain XAdES properties, suitably profiled for reducing the optionality as much as possible and referring to the forms that are specified in XAdES [1].

Clause 4 identifies the four conformance levels and shows how these levels might encompass the life cycle of the electronic signatures.

Clause 5 provides details on the way that the requirements will be presented throughout the present document.

Clause 6 profiles short-term related XAdES properties.

Clause 7 profiles a XAdES signature for which a Trust Service Provider has generated a trusted token (time-mark or time-stamp token) proving that the signature itself actually existed at a certain date and time.

Clause 8 profiles long-term related XAdES properties tackling the long term availability of the signature validation material.

Clause 9 long-term related XAdES properties tackling the long term availability and integrity of the signature validation material.

Informative Annex A highlits the most relevant changes introduced by the present specification with regards the ETSI TS 102 171 [i.9].

NOTE: The present document makes use of certain verbal forms (e.g. may, shall, shall not and should) as key words to signify requirements, conforming to ETSI Drafting Rules, clause 14a [i.8].

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references,only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are necessary for the application of the present document.

[1] EN 319 312-1: "XML Advanced Electronic signatures (XAdES). Part 1: Core specification".

[2] W3C Recommendation (April 2013): "XML Signature Syntax and Processing version 1.1".

[3] W3C Recommendation (March 2001): "Canonical XML Version 1.0".

[4] W3C Recommendation (July 2002): "Exclusive XML Canonicalization Version 1.0".

[5] W3C Recommendation (May 2008): "Canonical XML Version 1.1".

[6] W3C Recommendation (November 1999): "XSL Transformations (XSLT) Version 1.0".

[7] W3C Recommendation (November 2002): "XML-Signature XPath Filter 2.0".

[8] ETSI TS 102 176-1: "Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms".

[9] ECRYPT II (European Network of Excellence in Cryptology II): "ECRYPT II Yearly Report on Algorithms and Keysizes".

[10] IETF RFC 3986: "Uniform Resource Identifier (URI): Generic Syntax". January 2005

2.2 Informative references

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market.

[i.2] Commission Decision 2009/767/EC of 16 October 2009 amended by CD 2010/425/EU of 28 July 2010, setting out measures facilitating the use of procedures by electronic means through the "points of single contact" under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market.

[i.3] ETSI TS 102 231: "Electronic Signatures and Infrastructures (ESI); Provision of harmonized Trust-service status information".

[i.4] ETSI TS 101 533-1: "Electronic Signatures and Infrastructures (ESI); Data Preservation Systems Security; Part 1: Requirements for Implementation and Management".

[i.5] ETSI TS 102 640-1: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 1: Architecture".

[i.6] Commission Decision 2011/130/EU of 25 February 2011; establishing minimum requirements for the cross-border processing of documents signed electronically by competent authorities under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market (notified under document C(2011) 1081).

[i.7] ISO 8601:2004 (2004-12): "Data elements and interchange formats - Information interchange - Representation of dates and times".

[i.8] ETSI Drafting Rules (EDRs).

[i.9] ETSI TSI 103 171: “Electronic Signatures and Infrastructures (ESI); XAdES Baseline Profile”.

NOTE: Contained in the ETSI Directives: http://portal.etsi.org/Directives/home.asp

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

generator: any party which creates, or adds attributes to, a signature

NOTE: This may be the signatory or any party that initially verifies or further maintains the signature.

protocol element: element of the protocol which may be including data elements and / or elements of procedure

service element: element of service that may be provided using one or more protocol elements

NOTE: All alternative protocol elements provide an equivalent service to the users of the protocol.

trust service provider: body operating one or more (electronic) Trust Services (see [i.3])

verifier: entity that validates or verifies an electronic signature

3.2 Abbreviations

For the purposes of the present document, the [following] abbreviations [given in ... and the following] apply:

For the purposes of the present document, the abbreviations given in XAdES [1] and the following apply:

TSL Trust-service Status List (see [i.3])

4 Conformance Levels

The present document defines four conformance levels as indicated below.

Applications managing signatures conformant to requirements specified in clause 6 may claim **B-Level** (basic level) conformance.

Applications managing signatures conformant to **B-Level** and also conformant to requirements specified in clause 7 may claim **T-Level** (Trusted time for signature existence) conformance.

Applications managing signatures conformant to **T-Level** and also conformant to requirements specified in clause 8 of the present document may claim **LT-Level** (Long Term level) conformance.

Applications managing signatures conformant to **LT-Level** and also conformant to requirements specified in clause 9 of the present document may claim **LTA-Level** (Long Term with Archive time-stamps) conformance.

These conformance levels are defined for encompassing the life cycle of electronic signature, namely:

a) B-Level profiles incorporation of signed and some unsigned properties when the signature is actually generated.

NOTE 1: It is considered that this level is sufficient to conform to the Commission Decision 2011/130/EU of 25 February 2011 [i.6].

b) T-Level profiles the generation, for an existing signature, of a trusted token proving that the signature itself actually existed at a certain date and time.

c) LT-Level profiles the incorporation of all the material required for validating the signature in the signature. This level is understood to tackle the long term availability of the validation material.

d) LTA-Level profiles the incorporation of time-stamp tokens that allow validation of the signature long time after its generation. This level is understood to tackle the long term availability and integrity of the validation material.

NOTE 2: The levels b) to d) are appropriate where the technical validity of signature needs to be preserved for a period of time after signature creation where certificate expiration, revocation and/or algorithm obsolescence is of concern. The specific level applicable depends on the context and use case.

All conformance levels up to LTA use properties defined in XAdES [1].

When signed data is exchanged between parties the sender should use at least signatures conforming to a level that allows the relying parties to trust the signature at the time the exchange takes place.

NOTE 3: Archiving or preservation of electronic signatures over long term requires in general conformance to LTA level. The use of LTA-level is considered an appropriate preservation and transmission technique for signed data. Conformance to lower level is sufficient when combined with appropriate additional protection techniques such as use of systems compliant to TS 101 533-1 [i.4].

NOTE 4: The assessment of the effectiveness of other preservation and transmission techniques for signed data are out of the scope of the present document. The reader is advised to consider legal instruments in force and related standards such as TS 101 533-1 [i.4] or TS 102 640-1 [i.5] to evaluate their appropriateness.

5 General requirements

5.1 Algorithm requirements

Generators are referred to applicable national laws regarding algorithms and key lengths.

Generators are also recommended to take into account the latest version of TS 102 176-1 [8] for guidelines purposes and the latest ECRYPT2 D.SPA.x [9] yearly report for further recommendations, when selecting algorithms and key lengths.

MD5 algorithm shall not be used as digest algorithm.

5.2 Compliance requirements

Profiles in the present document define requirements for generators of XAdES signatures [1].

A verifier shall be able to accept a signature containing any elements/properties conformant to XAdES [1], but this profile does not specify any processing requirement on such elements/properties present in the signature as it is meant to be used together with a specification describing processing during signature validation.

Requirements are grouped in two different categories, each one having its corresponding identifier. Table 1 defines these categories and their identifiers.

Table 1: Requirement categories

Identifier	Requirement on generator
M	Generator shall include the element in the signature.
O	Generator may include the element in the signature.

Optional elements defined in XAdES [1] but not specified in the present document are treated as "O" as above.

Certain service elements may be provided by different protocol elements at user's choice. In these cases the semantics of M and O defined in table 1 depend on the requirement for the service element itself. Tables 2 and 3 (each one applies to a different requirement on the service element) define these semantics.

Table 2: Requirements for mandatory service with choices

Requirement Identifier for the Service / Protocol element	Requirement on generator
Service = M	Generator shall provide the service by including one protocol element chosen from the list of choices.
Protocol Choice = O	Generator may use this protocol element for providing the mandatory service elements.

Table 3: Requirements for optional service with choices

Requirement Identifier for the Service / Protocol element	Requirement on generator
Service = O	Generator may provide the service by including one protocol element chosen from the list of choices.
Protocol Choice = O	If the generator decides to provide the service, then it may use this protocol element.

The present document shows new requirements for each service and protocol element in tabular form. Below follows the structure of the table.

Table 4: Requirements for optional service with choices

Service / Protocol element	Reference	Requirement on generator	Additional requirements/notes
Service:			
Choice 1			
Choice 2			

Column **Service / Protocol element** will identify the service element or protocol element the requirement applies to. Service elements that may be implemented by different protocol elements (i.e. users may make a choice on several protocol elements) build tables with more than one row.

Column **Reference** will reference the relevant clause of the standard where the element is first defined. The reference is to XAdES [1], except where explicitly indicated otherwise.

Column **Requirement on generator** will contain an identifier of the requirement, as defined in table 1, bound to the corresponding protocol element for the generator.

Column **Notes/Additional requirements** will contain numbers referencing notes and/or letters referencing additional requirements. Both notes and additional requirements are listed below the table.

Profiles may be affected by applicable regulations; hence implementers should check any national regulation that may affect these profiles.

6 Requirements for B-Level Conformance

This clause defines requirements that XAdES signatures claiming conformance to the B-Level have to fulfil.

This clause actually profiles XAdES-BES (signatures that do not incorporate `xades:SignaturePolicyIdentifier`) and XAdES-EPES (signatures that do incorporate `xades:SignaturePolicyIdentifier`) signatures.

In consequence, the following XAdES properties are addressed directly in this clause: `xades:SigningCertificate`, `xadesv111:SigningCertificate`, `xades:SigningTime` and `xades:DataObjectFormat`. Further `xades:SignatureProductionPlace`, `xades:SignerRole`, `xadesenv111:SignerRole`, `xadesenv111:SignerRole`, `xades:AllDataObjectsTimeStamp`, `xades:IndividualDataObjectsTimeStamp`, `xades:SignaturePolicyIdentifier`, and `xades:CounterSignature` are also inherently addressed.

Clause 6.1 specifies the incorporation of the XAdES properties to the signature.

Clause 6.2 specifies additional requirements for some XML Sig [2] elements, namely: `ds:KeyInfo`, `ds:SignedInfo`, `ds:CanonicalizationMethod`, `ds:Reference` and `ds:Transform`.

Clause 6.3 specifies additional requirements for some of the XAdES [1] properties already mentioned. More specifically, this clause profiles `xadesenv111:SigningCertificate`, `xades:SigningTime` and `xades:DataObjectFormat`, and `xadesenv111:SignerRole`. No further requirements are defined by this profile for the rest of the XAdES properties already mentioned than those ones specified by XAdES [1].

6.1 Incorporation of XAdES qualifying properties to the signature

XAdES qualifying properties incorporation to the signature shall be direct as specified in [1], clause 6.3.

NOTE: This means that all the XAdES qualifying properties will remain within one single `xades:QualifyingProperties` element, which in turn will be the child of one `ds:Object` element within the signature; and that in consequence no `xades:QualifyingPropertiesReference` elements will be present.

6.2 Profile of elements defined in XML Signature

6.2.1 Placement of the signing certificate

Table 5

Service / Protocol element	XML SIG [2] Reference	Generator requirement	Additional requirements/notes
`ds:KeyInfo/X509Data/X509Certificate`	Clause 4.5.4	M	a, b

Additional requirements:

a) The generator shall include the signing certificate as content of `ds:KeyInfo/X509Data/X509Certificate` element.

b) In order to facilitate path-building, generators should include in the same `ds:KeyInfo/X509Data` element as in note a) all certificates not available to verifiers that can be used during path building. In the case of signature based on qualified certificates and whose verification is expected to be based on TSLs (in particular on Trusted Lists as defined in CD 2009/767/EC amended by CD 2010/425/EU [i.2]), the generator should include all intermediary certificates forming a chain between the signer certificate and a CA present in the TSL which are not available to verifiers.

NOTE 1: A certificate is considered available to the verifier, if reliable information about its location is known and allows automated retrieval of the certificate (for instance through an Authority Info Access Extension or equivalent information present in a TSL).

NOTE 2: In the general case, different verifiers can have different trust parameters and can validate the signer certificate through different chains. Therefore, generators may not know which certificates will be relevant for path building. However, in practice, such certificates can often clearly be identified. In this case, it is advised that generators include them unless they can be automatically retrieved by verifiers. In the specific case of a signature meant to be validated through TSL, it is advised to include at least the unavailable intermediary certificates up to but not including the CAs present in the TSLs, since the TSL is information that is shared globally by all verifiers.

6.2.2 Canonicalization of `ds:SignedInfo` element

Table 6

Service / Protocol element	Reference	Generator requirement	Additional requirements/notes
Service: canonicalization of `ds:SignedInfo` element		M	a
`ds:CanonicalizationMethod's Algorithm` attribute set to: "http://www.w3.org/2006/12/xml-c14n11"	XML Sig [2], clause 4.4.1 Can. XML V1.1 [5]	O	1
`ds:CanonicalizationMethod's Algorithm` attribute set to: "http://www.w3.org/2001/10/xml-exc-c14n#"	XML Sig [2], clause 4.4.1 Ex. Canon. [7]	O	2
`ds:CanonicalizationMethod's Algorithm` attribute set to: "http://www.w3.org/TR/2001/REC-xml-c14n-20010315"	XML Sig [2], clause 4.4.1 Can. XML V1.0 [3]	O	3
`ds:CanonicalizationMethod's Algorithm attribute` set to: "http://www.w3.org/2006/12/xml-c14n11#WithComments"	XML Sig [2], clause 4.4.1 Can. XML V1.1 [5]		a, 4, 7
`ds:CanonicalizationMethod's Algorithm` attribute set to: "http://www.w3.org/2001/10/xml-exc-c14n#WithComments"	XML Sig [2], clause 4.4.1 Ex. Canon. [7]		a, 5, 7
`ds:CanonicalizationMethod's Algorithm` attribute set to: "http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments"	XML Sig [2], clause 4.4.1 Can. XML V1.0 [3]		a, 6, 7

Additional requirement:

a) The generator should not use canonicalization algorithms "with comments".

NOTE 1: This URI value corresponds to Canonical XML v1.1 (omits comments).

NOTE 2: This URI value corresponds to Exclusive Canonicalization [4] (omits comments).

NOTE 3: This URI value corresponds to Canonical XML v1.0 (omits comments).

NOTE 4: This URI value corresponds to Canonical XML v1.1 (with comments).

NOTE 5: This URI value corresponds to Exclusive Canonicalization (with comments).

NOTE 6: This URI value corresponds to Canonical XML v1.0 (with comments).

NOTE 7: Support of canonicalization algorithms "with comments" is for residual interoperability in the signature verification process.

6.2.3 Profile of `ds:Reference` element

Table 7

Service / Protocol element	XML Sig Reference [2]	Generator requirement	Additional requirements/notes
`ds:Reference`	Clause 4.4.3	M	a, b

Additional requirements:

a) The generator shall create as many `ds:Reference` element as signed data objects (each one referencing one of them) plus one `ds:Reference` element referencing `xades:SignedProperties` element.

b) The `ds:Reference`'s `URI` attribute referencing signed data objects may have as values references that are or are not "same-document" references as defined in [10], section 4.4.

6.2.4 Transforms within ds:Reference element

Table 8

Service / Protocol element	Reference	Generator requirement	Additional requirements/ notes
Service: Transforms applicable within ds:Reference element		O	a, b
ds:Transform's Algorithm attribute set to: "http://www.w3.org/2000/09/xmldsig#base64"	XML Sig [2], clause 6.6.2	O	
ds:Transform's Algorithm attribute set to: "http://www.w3.org/TR/1999/REC-xpath-19991116"	XML Sig [2], clause 6.6.3	O	
ds:Transform's Algorithm attribute set to: "http://www.w3.org/2000/09/xmldsig#enveloped-signature"	XML Sig [2], clause 6.6.4	O	
ds:Transform's Algorithm attribute set to: "http://www.w3.org/TR/1999/REC-xslt-19991116"	XML Sig [2], clause 6.6.5 XSLT [6]	O	
ds:Transform's Algorithm attribute set to: "http://www.w3.org/2002/06/xmldsig-filter2"	XPathFilter 2 [7]	O	
ds:Transform's Algorithm attribute set to: "http://schemas.openxmlformats.org/package/2006/RelationshipTransform"		O	

Additional requirements:

a) Generator should limit the range of transforms used in the signatures to the ones identified in table 8 of the present document.

b) Requirements defined in clause 6.2.2 of the present document shall apply when ds:Transform's Algorithm attribute is set to any of the canonicalization algorithms identifiers mentioned in that clause.

6.3 Profile of XAdES elements

6.3.1 Profile of xadesenv111:SigningCertificate element

Table 9

Service / Protocol element	XAdES Reference [1]	Generator requirement	Additional requirements/notes
xadesenv111:SigningCertificate	Clause 6.2.2	M	a, b,1
xadesenv111:SigningCertificate/CertDigest	Clause 6.2.2	M	c
xadesenv111:SigningCertificate/IssuerSerial	Clause 6.2.2	M	d

Additional requirements:

a) Any new XAdES signature created after the publication of the present specification, and including xades:SigningCertificate shall not be conformant to the present specification. Legacy XAdES signatures, created before the date of publication of the present specification, and including xades:SigningCertificate property shall be considered as conformant to the present specification.

b) The generator shall not generate xadesenv111:Cert children's URI optional attribute.

b) xadesenv111:SigningCertificate/CertDigest element shall contain the digest value of the signing certificate present within ds:KeyInfo element and the identifier of the corresponding digest algorithm.

c) xadesenv111:SigningCertificate/IssuerSerial element shall contain textual representations of the issuer and the serial number of the signing certificate present within ds:KeyInfo element. The string representing the serial number shall contain the textual representation of this serial number field as specified in XAdES [1].

NOTE 1: The presence of the signing certificate within `ds:KeyInfo` ensures a way to locate it (on the basis of digest equality with the value within `xadesenv111:SigningCertificate/CertDigest`) within the signature.

EDITOR NOTE: feedback from stakeholders is requested on the solution proposed: define the new `xadesenv111:SigningCertificate` for acknowledging deprecation of `ds:X509IssuerSerial`, but keep `xades:SigningCertificate` for keeping backwards compatibility. The reason for defining the new `xadesenv111:SigningCertificate` signed property in the EN 319 132 Part 1 (XAdES core specification) is that XMLDSig in its version 1.1 [2], has deprecated the usage of `ds:X509IssuerSerial` element. The rationale for its deprecation is that some XML Schema validation tools do not deal with integer values that have more than 18 decimal digits. It is not uncommon that the randomly generated serial numbers need more than 18 digits.

6.3.2 Profile of `xades:SigningTime` element

Table 10

Service / Protocol element	XAdES Reference [1]	Generator requirement	Additional requirements/notes
`xades:SigningTime`	Clause 6.2.1	M	a

Additional requirement:

a) The generator shall include the claimed UTC time when the signature was generated as content of this element.

6.3.3 Profile of `xades:DataObjectFormat` element

Table 11

Service / Protocol element	XAdES Reference [1]	Generator requirement	Additional requirements/notes
`xades:DataObjectFormat`	Clause 6.2.4	M	a, 1
`xades:DataObjectFormat/Description`	Clause 6.2.4	O	
`xades:DataObjectFormat/ObjectIdentifier`	Clause 6.2.4	O	
`xades:DataObjectFormat/MimeType`	Clause 6.2.4	M	
`xades:DataObjectFormat/Encoding`	Clause 6.2.4	O	
`xades:DataObjectFormat's ObjectReference attribute`	Clause 6.2.4	M	

Additional requirement:

a) Implementations claiming conformance to the present document shall generate one `xades:DataObjectFormat` for each signed data object, except the `xades:SignedProperties` element.

NOTE 1: XAdES [1] specification establishes that this signed property "qualifies one specific signed data object". This is done by forcing that `ObjectReference` attribute refers to a `ds:Reference`. However XAdES does not mandate this `ds:Reference` to be a child of `ds:SignedInfo`; it actually could be a `ds:Reference` within a signed `ds:Manifest`, as the object referenced in this way is also a signed object.

6.3.4 Profile of `xadesenv111:SignerRole` element

Table 12

Service / Protocol element	XAdES Reference [1]	Generator requirement	Additional requirements/notes
`xadesenv111:SignerRole`	Clause 6.2.6.2	O	a,1

Additional requirements:

a) Any new XAdES signature created after the publication of the present specification, and including `xades:SignerRole` shall not be conformant to the present specification. Legacy XAdES signatures, created before the date of publication of the present specification, and including `xades:SignerRole` property shall be considered as conformant to the present specification.

EDITOR NOTE: feedback from stakeholders is requested on the solution proposed: define the new `xadesenv111:SignerRole` for satisfying requests of allowing things like signed SAML assertions in this element. See XAdES[1] for details.

7 Requirements for T-Level Conformance

This clause defines those requirements that XAdES signatures conformant to B-Level, have to fulfil to also be conformant to T-Level. In consequence, XAdES signatures claiming conformance to the T-Level of the present profile shall be built on signatures conformant to the B-Level.

A XAdES signature conformant to T-Level shall be a signature conformant to B-Level for which a Trust Service Provider has generated a trusted token (time-mark or time-stamp token) proving that the signature itself actually existed at a certain date and time.

NOTE: XAdES signatures conformant to T-Level of the present specification are, in consequence, XAdES-T signatures suitably profiled as per the requirements defined in this clause.

Table 12 further profiles the provision of the trusted token that proves existence of the signature at a certain date and time.

Table 13

Service / Protocol element	XAdES Reference [1]	Generator requirement	Additional requirements/notes
Service: trusted time for existence of the signature		M	
`xades:SignatureTimeStamp`	Clause 6.3	O	a, b
`Time-mark`	Clause 6.3	O	c

Additional requirements:

a) The present profile recommends usage of time-stamps as attestation of the time for existence of the signature instead of time-marks.

b) A XAdES signature claiming conformance to the T-Level may contain several `xades:SignatureTimeStamp` elements. Each `xades:SignatureTimeStamp` element shall contain only one time-stamp token.

c) If a time-mark is used, then no additional property is incorporated in the signature. It is the responsibility of the TSP generating the time-mark to provide the needed trust on the signature time.

8 Requirements for LT-Level Conformance

This clause defines those requirements that XAdES signatures conformant to T-Level, have to fulfil to also be conformant to LT-Level. In consequence, XAdES signatures claiming conformance to the LT-Level of the present profile shall be built on signatures conformant to the T-Level.

8.1 Profile of XAdES elements

XAdES signatures conformant to LT-Level shall not incorporate any of the following XAdES unsigned attributes: `xades:CompleteCertificateRefs`, `xades:CompleteRevocationRefs`,

`xades:AttributeCertificateRefs`, `xades:AttributeRevocationRefs`, `xades:SigAndRefsTimeStamp`, and `xades:RefsOnlyTimeStamp`.

NOTE: The requirements above are meant to highly reduce optionality.

XAdES signatures conformant to LT-Level are built by direct incorporation to XAdES-T signatures conformant to the T-Level, of XAdES unsigned properties containing values of certificates and values of certificate status. In consequence, this clause defines additional specific requirements for the following unsigned XAdES properties: `xades:CertificateValues`, `xades:RevocationValues`, `xades:AttrAuthoritiesCertValues`, `xades:AttributeRevocationValue` , and `xadesv141:TimeStampValidationData`.

Clauses below define additional requirements for these XAdES unsigned properties.

8.1.1 Profile of `xades:CertificateValues` property

Table 14

Service / Protocol element	XAdES Reference [1]	Generator requirement	Additional requirements/notes
Service: certificate values	Clause 6.4.1	M	
`xades:CertificateValues`	Clause 6.4.1	O	a, b, c

Additional requirements:

a) Implementations claiming conformance to this profile shall include in this property the set of certificate values that, in addition to the certificate values present within `ds:KeyInfo` element, build up the full set of certificates (including the trust anchor when it is available in the form of a certificate) used to validate the signature.

b) In situations different from those ones identified in clause 6.2.1 of the present document, requirements a) and b), applications should include certificate values within `xades:CertificateValues` property.

c) Duplication of certificate values within the signature should be avoided.

8.1.2 Profile of `xades:RevocationValues` property

Table 15

Service / Protocol element	XAdES Reference [1]	Generator requirement	Additional requirements/notes
Service: revocation values	Clause 6.4.2	M	
`xades:RevocationValues`	Clause 6.4.2	O	a, b, c

Additional requirements:

a) Implementations claiming conformance to this profile shall include in this property the set of revocation values that, in addition to the revocation values present within `ds:KeyInfo` element, build up the full set of revocation values used to validate the signature.

b) Applications should include certificate status values within `xades:RevocationValues` property instead within `ds:KeyInfo` element.

c) Duplication of revocation values within the signature should be avoided.

8.1.3 Profile of `xades:AttrAuthoritiesCertValues` property

If the signature contains attribute certificates or signed assertions within `xades:SignerRole` or `xadesenv111:SignerRole` signed properties, implementations claiming conformance to this profile shall include in this property the Attribute Authorities certificates values (or the certificates values of the entities signing the signed

assertions) and the set of CA certificate values that, in addition to the rest of certificate values present in the signature, build up the full set of certificates required for validating the attribute certificates or signed assertions.

8.1.4 Profile of `xades:AttributeRevocationValues` property

If the signature contains attribute certificates or signed assertions within `xades:SignerRole` or `xadesenv111:SignerRole` signed properties, implementations claiming conformance to this profile shall include in this property the set of revocation values that, in addition to the rest of revocation values present in the signature, are used for validating the attribute certificates or the signed assertions.

8.1.5 Validation material for time-stamp tokens

This clause further profiles the incorporation of the validation material for time-stamp tokens within XAdES signatures compliant with LT-Level.

Table 16

Service / Protocol element	XAdES Reference [1]	Generator requirement	Additional requirements/notes
Service: validation data for time-stamp tokens		M	1
`xadesv141:TimeStampValidationData`	Clause 6.5.1	O	2
`embedded in time-stamp token itself`		O	

NOTE 1: This ensures that the signature profiled actually contains all the validation material needed.

NOTE 2: Although this profile allows incorporation of the validation material within the time-stamp token itself, within the new XAdES element, or within both, applications should implement support for `xadesv141:TimeStampValidationData`.

9 Requirements for LTA-Level Conformance

This clause defines those requirements that XAdES signatures conformant to LT-Level, have to fulfil for also be conformant to LTA-Level. In consequence, XAdES signatures claiming conformance to the LTA-Level of the present profile shall be built on signatures conformant to the LT-Level.

A XAdES signature conformant to LTA-Level shall be a signature conformant to LT-Level to which one or more `xades:ArchiveTimeStamp` (or `xadesv141:ArchiveTimeStamp`) have been directly incorporated.

NOTE 1: This conformance level specifies a profile for XAdES-A signatures.

NOTE 2: As stated in XAdES [1], XAdES-A form may help to validate the signature beyond any event that may limit its validity.

Table 17

Service / Protocol element	XAdES Reference [1]	Generator requirement	Additional requirements/notes
Service: add archive time-stamp		M	
`xadesv141:ArchiveTimeStamp`	6.5.2	M	a, b, c, d, e

Additional requirements:

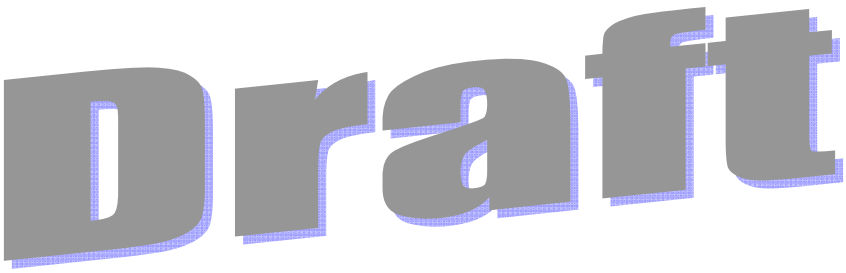
a) Applications claiming conformance to this profile shall consider conformant to LTA-level any XAdES signature including one or more `xades:ArchiveTimeStamp` properties if it fulfils all the requirements specified in the clauses above and it may be ascertained that all the time-stamp tokens contained within these `xades:ArchiveTimeStamp` properties were generated before 2013/01/01T00:00:00 UTC.

b) Signatures created at or after 2013/01/01T00:00:00 UTC claiming conformance to LTA-level shall incorporate one or more `xadesv141:ArchiveTimeStamp` properties. They shall not incorporate any `xades:ArchiveTimeStamp` property.

c) `xades:ArchiveTimeStamp` and `xadesv141:ArchiveTimeStamp` within signatures conformant to the LTA-Level may contain more than one time-stamp token issued by different TSAs.

d) Before generating and incorporating a new `xadesv141:ArchiveTimeStamp` property, applications claiming conformance to this profile, shall include all the validation material required for verifying the electronic signature. This validation material includes all the certificates and all certificate status information (like CRLs or OCSP responses) required for:

- validating the signing certificate;
- validating any attribute certificate or signed assertion present in the signature; and
- validating the signing certificate of any previous time-stamp token already incorporated in the signature within any XAdES time-stamp token container property (including, of course, `xades:ArchiveTimeStamp` and/or `xadesv141:ArchiveTimeStamp`).



Annex E (informative): Change History

date	Version	Information about changes
November 2013	V0.0.3	Use of `xadesenv111:SigningCertificate` and `xadesenv111:SignerRole` instead `xades:SigningCertificate` and `xades:SignerRole`. Incorporate mention to the signed assertions as per ETSI 319 132-1. Also deleted clause 9.1 on transition strategy as this period finalized in January 2013.

History

Document history		
<Version>	<Date>	<Milestone>
0.0.4	2013-11	Stable draft for public comments.