Draft **ETSI EN 319 132-2** V1.0.0 (2015-06)

EUROPEAN STANDARD

**Electronic Signatures and Infrastructures (ESI);
XAdES digital signatures;
Part 2: Extended XAdES signatures**

Reference

DEN/ESI-0019132-2

Keywords

electronic signature, security, XAdES, XML

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

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (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:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Copyright Notification

ETSI

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), and is now submitted for the combined Public Enquiry and Vote phase of the ETSI standards EN Approval Procedure.

The present document is part 2 of a multi-part deliverable covering XAdES digital signatures. Full details of the entire series can be found in 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

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Introduction

Electronic commerce has emerged as a frequent way of doing business between companies across local, wide area and global networks. Trust in this way of doing business is essential for the success and continued development of electronic commerce. It is therefore important that companies using this electronic means of doing business have suitable security controls and mechanisms in place to protect their transactions and to ensure trust and confidence with their business partners. In this respect digital signatures are an important security component that can be used to protect information and provide trust in electronic business.

The present document is intended to cover digital signatures supported by PKI and public key certificates, and aims to meet the general requirements of the international community to provide trust and confidence in electronic transactions, including, amongst other, applicable requirements from Regulation (EU) No 910/2014 [i.1].

The present document can be used for any transaction between an individual and a company, between two companies, between an individual and a governmental body, etc. The present document is independent of any environment. It can be applied to any environment e.g. smart cards, GSM SIM cards, special programs for electronic signatures, etc.

The present document is part of a rationalized framework of standards (see ETSI TR 119 000 [i.5]). See ETSI TR 119 100 [i.6] for getting guidance on how to use the present document within the aforementioned framework.

1 Scope

The present document specifies XAdES digital signatures. XAdES signatures are built on XML digital signatures [i.4], by incorporation of signed and unsigned qualifying properties, which fulfil certain common requirements (such as the long term validity of digital signatures, for instance) in a number of use cases.

The present document specifies a number of XAdES signature levels, addressing incremental requirements to maintain the validity of the signatures over the long term, in a way that a certain level always addresses all the requirements addressed at levels that are below it. These XAdES extended signatures offer a higher degree of optionality than the XAdES baseline signatures specified ETSI EN 319 132-1 [1].

The present document aims at supporting electronic signatures in different regulatory frameworks.

> NOTE: Specifically but not exclusively, XAdES digital signatures specified in the present document aim at supporting electronic signatures, advanced electronic signatures, qualified electronic signatures, electronic seals, advanced electronic seals, and qualified electronic seals as per Regulation (EU) No 910/2014 [i.1].

2 References

2.1 Normative 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.

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

[1] ETSI EN 319 132-1: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures".

2.2 Informative 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.

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

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] Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. OJ L 257, 28.08.2014, p. 73-114.

[i.2] ETSI TR 119 001: "Electronic Signatures and Infrastructures (ESI); Definitions and abbreviations".

[i.3] ETSI TS 101 903: "Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES)".

[i.4] W3C Recommendation: "XML-Signature Syntax and Processing. Version 1.1".

[i.5]   ETSI TR 119 000: "Electronic Signatures and Infrastructures (ESI); Rationalized structure for Electronic Signature Standardization".

[i.6]   ETSI TR 119 100: "Electronic Signatures and Infrastructures (ESI); Business Driven Guidance for Signature Creation and Validation".

3   Definitions, abbreviations and terminology

3.1   Definitions

For the purposes of the present document, the terms and definitions given in ETSI TR 119 001 [i.2] and ETSI EN 319 132-1 [1], apply.

3.2   Abbreviations

For the purposes of the present document, the following abbreviations apply:

EU   European Union
GSM   Global System for Mobile communications
OCSP   Online Certificate Status Protocol
PKI   Public Key Infrastructure
SIM   Subscriber Identity Module
SPO   Service Provision Option
TSA   Time-Stamping Authorities
URI   Uniform Resource Identifier
XML   eXtensible Markup Language

3.3   Terminology

The present document uses the term "qualifying property" for denoting a XML element that qualifies the signature, the signed data objects, or the signer.

The present document uses the term "element" exclusively for denoting XML elements.

The present document uses the terms "container" or "element" for denoting XML elements that are containers of qualifying properties (for instance `QualifyingProperties`, `SignedProperties`, or `UnsignedProperties`).

The present document uses the term "attribute" exclusively for denoting XML attributes of XML elements. Consequently, a qualifying property, being a XML element, can have (XML) attributes.

The present document uses the term "child element" exclusively in the context of XML content, for denoting an XML element that is a child element of another XML element.

4   Additional XAdES levels without references to validation data

4.1   Overview

The present document specifies a number of additional levels for XAdES.

Each level is generated by a different combination of the XAdES qualifying properties specified in ETSI EN 319 312-1 [1], and incorporated to the XAdES signatures using one of the two mechanisms (direct or indirect incorporation) described in clause 4.4 of ETSI EN 319 312-1 [1].

NOTE 1:   Clause 4.3 defines four XAdES levels namely the XAdES-E-BES, XAdES-E-EPES, XAdES-E-T, and XAdES-E-A built on XAdES-E-T. Normative Annex A defines levels of XAdES signatures incorporating qualifying properties that encapsulate references to validation data and qualifying properties that encapsulate time-stamp tokens on them.

NOTE 2:   Names of XML elements in the namespace whose URI is http://www.w3.org/2000/09/xmldsig# will be preceded in the present document by prefix `ds`. No other prefixes will be used in the present document for identifying XAdES containers and/or XAdES qualifying properties, as their usage is not required for unambiguously identifying the referenced XAdES container or XAdES qualifying property, regardless of the namespace where they have been defined.

NOTE 3:   The requirements on the presence and cardinality of the attributes for each XAdES signature level are expressed in tables whose formats and semantics are as specified in clause 6.2.2 of ETSI EN 319 132-1 [1].

4.2   General requirements

XAdES qualifying properties obsoleted by ETSI EN 319 132-1 [1] do not appear in the tables. Their cardinality shall be 0 and consequently, they shall not be incorporated in the signature.

Any XAdES signature of any of the levels specified in the present document shall contain at least one of the following components with the specified contents:

- The `SigningCertificateV2` signed qualifying property.

- The `ds:KeyInfo` element. If the `SigningCertificateV2` qualifying property is incorporated to the signature, no restrictions apply to this 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 certificate is actually signed.

NOTE: Signing the whole `ds:KeyInfo` locks the element: any addition of a certificate or validation data would make signature validation fail. Applications can, alternatively, use XPath transforms for signing at least the signing certificate, leaving the `ds:KeyInfo` element open for addition of new data after signing.

4.3   XAdES-E-BES, XAdES-E-EPES, XAdES-E-T signatures, and XAdES-E-A signatures built on XAdES-E-T signatures

XAdES-E-BES, XAdES-E-EPES, XAdES-E-T, and XAdES-E-A built on XAdES-E-T signatures shall be XAdES signatures whose qualifying properties satisfy the requirements specified in the present clause.

XAdES-E-EPES signatures are built on XAdES-E-BES signatures by adding one `SignaturePolicyIdentifier` qualifying property.

XAdES-E-T signatures are built on XAdES-E-BES and XAdES-E-EPES signatures by adding one or more `SignatureTimeStamp` qualifying properties.

XAdES-E-A signatures are built on XAdES-E-T, XAdES-E-C, XAdES-E-X (of Type 1 and of Type 2), XAdES-E-X-Long, and XAdES-E-X-L (of Type 1 and of Type 2) signatures.

Annex A specifies XAdES-E-C, XAdES-E-X (of Type 1 and of Type 2), XAdES-E-X-Long, and XAdES-E-X-L (of Type 1 and of Type 2) signatures, and XAdES-E-A signatures built on them.

Table 1: Requirements for XAdES-E-BES, XAdES-E-EPES, XAdES-E-T, and XAdES-E-A built on XAdES-E-T

Elements/Qualifying properties/Services	Presence in E-BES level	Presence in E-EPES level	Presence in E-T level	Presence in E-A level built on E-T level	Cardinality	Additional notes and requirements	Reference
`SigningTime`	may be present	may be present	may be present	may be present	0 or 1		ETSI EN 319 132-1 [1], clause 5.2.1
`SigningCertificateV2`	conditioned presence	conditioned presence	conditioned presence	conditioned presence	0 or 1	a, b	ETSI EN 319 132-1 [1], clause 5.2.2
`CommitmentTypeIndication`	may be present	may be present	may be present	may be present	≥ 0		ETSI EN 319 132-1 [1], clause 5.2.3
`DataObjectFormat`	may be present	may be present	may be present	may be present	≥ 0		ETSI EN 319 132-1 [1], clause 5.2.4
`SignatureProductionPlaceV2`	may be present	may be present	may be present	may be present	0 or 1		ETSI EN 319 132-1 [1], clause 5.2.5
`SignerRoleV2`	may be present	may be present	may be present	may be present	0 or 1		ETSI EN 319 132-1 [1], clause 5.2.6
`CounterSignature`	may be present	may be present	may be present	may be present	≥ 0		ETSI EN 319 132-1 [1], clause 5.2.7.2
`AllDataObjectsTimeStamp`	may be present	may be present	may be present	may be present	≥ 0	1	ETSI EN 319 132-1 [1], clause 5.2.8.1
`IndividualDataObjectsTimeStamp`	may be present	may be present	may be present	may be present	≥ 0	1	ETSI EN 319 132-1 [1], clause 5.2.8.2
`SignaturePolicyIdentifier`	*	shall be present	may be present	may be present	E-EPES: 1 E-BES, E-T, E-A: 0 or 1	2, 3	ETSI EN 319 132-1 [1], clause 5.2.9
`SignaturePolicyStore`	*	conditioned presence	conditioned presence	conditioned presence	0 or 1	c	ETSI EN 319 132-1 [1], clause 5.2.10
`SignatureTimeStamp`	*	*	shall be present	shall be present	E-BES, E-EPES: ≥ 0 E-T, E-A: ≥ 1	d, e 1, 4	ETSI EN 319 132-1 [1], clause 5.3
`CertificateValues`	*	*	*	conditioned presence	0 or 1	f, g	ETSI EN 319 132-1 [1], clause 5.4.1
`AttrAuthoritiesCertValues`	*	*	*	conditioned presence	0 or 1	f, h	ETSI EN 319 132-1 [1], clause 5.4.3
`RevocationValues`	*	*	*	conditioned presence	0 or 1	i, j	ETSI EN 319 132-1 [1], clause 5.4.2
`AttributeRevocationValues`	*	*	*	conditioned presence	0 or 1	i, k	ETSI EN 319 132-1 [1], clause 5.4.4
Service: incorporation of validation data for electronic time-stamps	*	*	*	shall be provided	-	l, m	ETSI EN 319 132-1 [1], clause 5.5.1
SPO: `TimeStampValidationData`	*	*	*	conditioned presence	≥ 0	m	ETSI EN 319 132-1 [1], clause 5.5.1
SPO: certificate and revocation values embedded in the electronic time-stamp itself	*	*	*	conditioned presence	≥ 0	m	ETSI EN 319 132-1 [1], clause 5.5.1

Elements/Qualifying properties/Services	Presence in E-BES level	Presence in E-EPES level	Presence in E-T level	Presence in E-A level built on E-T level	Cardinality	Additional notes and requirements	Reference
ArchiveTimeStamp	*	*	*	shall be present	E-BES, E-EPES, E-T: ≥ 0 E-A: ≥ 1	n, o, p	ETSI EN 319 132-1 [1], clause 5.5.2
RenewedDigest	*	*	*	conditioned presence	≥ 0	q	ETSI EN 319 132-1 [1], clause 5.5.3
CompleteCertificateRefsV2	*	*	*	*	0 or 1	r	ETSI EN 319 132-1 [1], clause A.1.1
AttributeCertificateRefsV2	*	*	*	*	0 or 1	r, s	ETSI EN 319 132-1 [1], clause A.1.3
CompleteRevocationRefs	*	*	*	*	0 or 1		ETSI EN 319 132-1 [1], clause A.1.2
AttributeRevocationRefs	*	*	*	*	0 or 1	r	ETSI EN 319 132-1 [1], clause A.1.4
RefsOnlyTimeStampV2	*	*	*	*	≥ 0	1	ETSI EN 319 132-1 [1], clause A.1.5.2
SigAndRefsTimeStampV2	*	*	*	*	≥ 0	1	ETSI EN 319 132-1 [1], clause A.1.5.1

Additional requirements:

a) Requirement for `SigningCertificateV2`. The `SigningCertificateV2` qualifying property shall be present if the signing certificate is not present within the `ds:KeyInfo` element, or if the signing certificate is present within the `ds:KeyInfo` element but it is not signed by the signature. Otherwise the `SigningCertificateV2` qualifying property may be absent.

b) Requirement for `SigningCertificateV2`. The references to certificates should not include the `IssuerSerialV2` element.

c) Requirement for `SignaturePolicyStore`. This qualifying property may be incorporated into the XAdES signature only if the `SignaturePolicyIdentifier` is also incorporated and it contains the `SigPolicyHash` element with the digest value of the signature policy document. Otherwise the `SignaturePolicyStore` shall not be incorporated into the XAdES signature.

d) Requirement for `SignatureTimeStamp`. Each `SignatureTimeStamp` element may contain one or more electronic time-stamps issued by different TSAs.

e) Requirement for `SignatureTimeStamp`. The electronic time-stamps encapsulated within the `signature-time-stamp` attributes shall be created before the signing certificate has been revoked or has expired.

f) Requirement for `CertificateValues` and `AttrAuthoritiesCertValues`. Duplication of certificate values within the signature should be avoided.

g) Requirement for incorporation of `CertificateValues`. For generating a XAdES-E-A signature, the incorporation of `CertificateValues` shall be determined by requirements specified in ETSI EN 319 132-1 [1], clauses 5.5.2.2 and 5.5.2.3, steps 4.a of the algorithms specified for computing the input to the electronic time-stamp's message imprint.

h) Requirement for incorporation of `AttrAuthoritiesCertValues`. For generating a XAdES-E-A signature, the incorporation of `AttrAuthoritiesCertValues` shall be determined by requirements specified in ETSI EN 319 132-1 [1], clauses 5.5.2.2 and 5.5.2.3, steps 4.c of the algorithms specified for computing the input to the time-stamp token's message imprint.

i) Requirement for `RevocationValues` and `AttributeRevocationValues`. Duplication of revocation values within the signature should be avoided.

j) Requirement for incorporation of `RevocationValues`. For generating a XAdES-E-A signature, the incorporation of `RevocationValues` shall be determined by requirements specified in ETSI EN 319 132-1 [1], clauses 5.5.2.2 and 5.5.2.3, steps 4.b of the algorithms specified for computing the input to the time-stamp token's message imprint.

k) Requirement for incorporation of `AttributeRevocationValues`. For generating a XAdES-E-A signature, the incorporation of `AttributeRevocationValues` shall be determined by requirements specified in ETSI EN 319 132-1 [1], clauses 5.5.2.2 and 5.5.2.3, steps 4.d of the algorithms specified for computing the input to the time-stamp token's message imprint.

l) Requirement for service "incorporation of validation data for electronic time-stamps". The validation data for electronic time-stamps shall be present within the `TimeStampValidationData` qualifying property or embedded in the electronic time-stamp itself.

m) Requirement for service "incorporation of validation data for electronic time-stamps" and its two options. The validation data for electronic time-stamps should be included in the `TimeStampValidationData` qualifying property.

n) Requirement for `ArchiveTimeStamp` defined in namespace whose URI is "http://uri.etsi.org/01903/v1.4.1#". Each `ArchiveTimeStamp` qualifying property defined in namespace whose URI is http://uri.etsi.org/01903/v1.4.1# may contain more than one electronic time-stamp issued by different TSAs.

o) Requirement for `ArchiveTimeStamp` defined in namespace whose URI is "http://uri.etsi.org/01903/v1.4.1#". XAdES-E-A signatures shall incorporate new archival electronic time-stamps to a previously existing XAdES-E-A signature, encapsulating these electronic time-stamps in new `ArchiveTimeStamp` qualifying properties defined in namespace whose URI is http://uri.etsi.org/01903/v1.4.1#.

p) Requirement for `ArchiveTimeStamp` defined in namespace whose URI is "http://uri.etsi.org/01903/v1.4.1#". Before generating and incorporating a new `ArchiveTimeStamp` qualifying property defined in namespace whose URI is http://uri.etsi.org/01903/v1.4.1#, all the validation material required for validating the XAdES signature shall be included. This validation material shall include all the certificates and all certificate status information (like CRLs or OCSP responses) required for:

- validating the signing certificate;

- validating the signing certificate of any countersignature incorporated into the signature;

- validating any attribute certificate or signed assertion present in the signature; and

- validating the signing certificate of any previous electronic time-stamp already incorporated into the signature within any XAdES electronic time-stamp container qualifying property (including `ArchiveTimeStamp` qualifying property defined in namespace whose URI is http://uri.etsi.org/01903/v1.4.1#).

q) Requirement for `RenewedDigest`. If the XAdES signature signs external data objects through a signed `ds:Manifest`, and some of the digest algorithms used for computing some of the digest values within the aforementioned `ds:Manifest` is suspected to become weak enough as to represent a threat, the `RenewedDigest` element should be used to counter this threat.

r) Requirement for `CompleteCertificateRefsV2`, and `AttributeCertificateRefsV2`. The references to certificates should not include the `IssuerSerialV2` element.

s) The `AttributeCertificateRefsV2` and `AttributeRevocationRefs` qualifying properties may be used when at least an attribute certificate or a signed assertion is incorporated into the XAdES signature. Otherwise, `AttributeCertificateRefsV2` and `AttributeRevocationRefs` attributes shall not be used.

NOTE 1: On `SignatureTimeStamp`, `IndividualDataObjectsTimeStamp`, `AllDataObjectsTimeStamp`, `RefsOnlyTimeStampV2`, `SigAndRefsTimeStampV2`. Several instances of these qualifying properties can be incorporated into the XAdES signature, coming from different TSAs.

NOTE 2: On `SignaturePolicyIdentifier`. The semantics of the signed data objects of XAdES-E-BES, XAdES-E-T, and XAdES-E-A signatures, or their context can implicitly indicate a signature policy.

NOTE 3: On `SignaturePolicyIdentifier`. The signature policy can establish specific requirements for other qualifying properties.

NOTE 4: On `SignatureTimeStamp`. `SignatureTimeStamp` qualifying property provides the initial steps towards providing long-term validity.

5   Legacy signatures

When new qualifying properties are incorporated to legacy XAdES 101 903 signatures [i.3], these qualifying properties shall comply with ETSI EN 319 312-1 [1].

Annex A (normative):
XAdES signature levels with references to validation data

A.1   XAdES-E-C, XAdES-E-X, XAdES-E-X-Long and XAdES-E-X-L signatures

The present clause specifies four XAdES signature levels that incorporate references to validation data, namely: XAdES-E-C, XAdES-E-X, XAdES-E-X-Long and XAdES-E-X-L.

XAdES-E-C signatures are built on XAdES-E-T signatures by adding qualifying properties containing references to certificates and references to certificate status data values.

XAdES-E-X signatures are built on XAdES-E-C signatures by adding one or more qualifying properties containing one or more electronic time-stamps as indicated in table A.1.

XAdES-E-X-Long signatures are built on XAdES-E-C signature by adding qualifying properties that contain certificates and revocation values as indicated in table A.1.

XAdES-E-X-L signatures are built on XAdES-E-X signatures by adding qualifying properties that contain certificates and revocation values as indicated in table A.1.

Some cells in column "additional requirements and notes" of table A.1 contain the text "as in table 1". This means that the additional requirements and notes from table 1 also apply to the element or service specified in the corresponding row, for the levels specified in table A.1.

Table A.1: Requirements for XAdES-E-C, XAdES-E-X, XAdES-E-X-Long and XAdES-E-X-L signatures

Elements/Qualifying properties/Services	Presence in E-C level	Presence in E-X level	Presence in E-X-Long level	Presence in E-X-L level	Cardinality	Additional notes and requirements	Reference
SigningTime	may be present	may be present	may be present	may be present	0 or 1		ETSI EN 319 132-1 [1], clause 5.2.1
SigningCertificateV2	conditioned presence	conditioned presence	conditioned presence	conditioned presence	0 or 1	As in table 1	ETSI EN 319 132-1 [1], clause 5.2.2
CommitmentTypeIndication	may be present	may be present	may be present	may be present	≥ 0		ETSI EN 319 132-1 [1], clause 5.2.3
DataObjectFormat	may be present	may be present	may be present	may be present	≥ 0		ETSI EN 319 132-1 [1], clause 5.2.4
SignatureProductionPlaceV2	may be present	may be present	may be present	may be present	0 or 1		ETSI EN 319 132-1 [1], clause 5.2.5
SignerRoleV2	may be present	may be present	may be present	may be present	0 or 1		ETSI EN 319 132-1 [1], clause 5.2.6
CounterSignature	may be present	may be present	may be present	may be present	≥ 0		ETSI EN 319 132-1 [1], clause 5.2.7.2
AllDataObjectsTimeStamp	may be present	may be present	may be present	may be present	≥ 0	As in table 1	ETSI EN 319 132-1 [1], clause 5.2.8.1
IndividualDataObjectsTimeStamp	may be present	may be present	may be present	may be present	≥ 0	As in table 1	ETSI EN 319 132-1 [1], clause 5.2.8.2
SignaturePolicyIdentifier	may be present	may be present	may be present	may be present	Built on E-EPES: 1 / Not built on E-EPES: 0	As in table 1	ETSI EN 319 132-1 [1], clause 5.2.9
SignaturePolicyStore	conditioned presence	conditioned presence	conditioned presence	conditioned presence	0 or 1	As in table 1	ETSI EN 319 132-1 [1], clause 5.2.10
SignatureTimeStamp	shall be present	shall be present	shall be present	shall be present	≥ 1	As in table 1	ETSI EN 319 132-1 [1], clause 5.3
CompleteCertificateRefsV2	shall be present	shall be present	shall be present	shall be present	1	a, b, 1	ETSI EN 319 132-1 [1], clause A.1.1
AttributeCertificateRefsV2	conditioned presence	conditioned presence	conditioned presence	conditioned presence	0 or 1	a, b, c	ETSI EN 319 132-1 [1], clause A.1.3
CompleteRevocationRefs	shall be present	shall be present	shall be present	shall be present	1	b, 1	ETSI EN 319 132-1 [1], clause A.1.2
AttributeRevocationRefs	conditioned presence	conditioned presence	conditioned presence	conditioned presence	0 or 1	b, d	ETSI EN 319 132-1 [1], clause A.1.4
RefsOnlyTimeStampV2	*	shall be present in E-X Type 2	*	shall be present in E-X-L Type 2	E-C, E-X-Long, E-X Type1, E-X-L Type 1: ≥ 0 / E-X Type 2, E-X-L Type 2: ≥ 1	As in table 1	ETSI EN 319 132-1 [1], clause A.1.5.2

Elements/Qualifying properties/Services	Presence in E-C level	Presence in E-X level	Presence in E-X-Long level	Presence in E-X-L level	Cardinality	Additional notes and requirements	Reference
SigAndRefsTimeStampV2	*	shall be present in E-X Type 1	*	shall be present in E-X-L Type 1	E-C, E-X-Long, E-X Type 2, E-X-L Type 2: ≥ 0 E-X Type 1, E-X-L Type 1: ≥ 1	As in table 1	ETSI EN 319 132-1 [1], clause A.1.5.1
CertificateValues	*	*	conditioned presence	conditioned presence	0 or 1	e, i	ETSI EN 319 132-1 [1], clause 5.4.1
RevocationValues	*	*	conditioned presence	conditioned presence	0 or 1	f, j	ETSI EN 319 132-1 [1], clause 5.4.2
AttrAuthoritiesCertValues	*	*	conditioned presence	conditioned presence	0 or 1	g, i	ETSI EN 319 132-1 [1], clause 5.4.3
AttributeRevocationValues	*	*	conditioned presence	conditioned presence	0 or 1	h, j	ETSI EN 319 132-1 [1], clause 5.4.4
Service: incorporation of validation data for electronic time-stamps	*	*	*	*	-	As in table 1	ETSI EN 319 132-1 [1], clause 5.5.1
SPO: TimeStampValidationData	*	*	*	*	≥ 0	As in table 1	ETSI EN 319 132-1 [1], clause 5.5.1
SPO: certificate and revocation values embedded in the electronic time-stamp itself	*	*	*	*	≥ 0	As in table 1	ETSI EN 319 132-1 [1], clause 5.5.1
ArchiveTimeStamp	*	*	*	*	≥ 0		ETSI EN 319 132-1 [1], clause 5.5.2
RenewedDigest	*	*	*	*	≥ 0		ETSI EN 319 132-1 [1], clause 5.5.3

Additional requirements:

a) Requirement for `CompleteCertificateRefsV2`, and `AttributeCertificateRefsV2`. The references to certificates should not include the `IssuerSerialV2` element.

b) Requirement for `CompleteCertificateRefsV2`, `AttributeCertificateRefsV2`, `CompleteRevocationRefs`, and `AttributeRevocationRefs`. In case of direct trust, i.e. when the signing certificate contains the trust anchor public key, XAdES-E-C signatures and the rest of XAdES signature levels specified in table A.1 shall not be generated. See note for rationale.

c) Requirement for `AttributeCertificateRefsV2`. This qualifying property may be incorporated into the XAdES signature only if the XAdES signature incorporates attribute certificates or signed assertions within the `SignerRoleV2` qualifying property. Otherwise it shall not be incorporated into the XAdES signature.

d) Requirement for `AttributeRevocationRefs`. This qualifying property may be incorporated into the XAdES signature only if the XAdES signature incorporates attribute certificates or signed assertions within the `SignerRoleV2` qualifying property. Otherwise it shall not be incorporated into the XAdES signature.

e) Requirement for `CertificateValues`. If a XAdES-E-X-Long signature or a XAdES-E-X-L signature is generated, `CertificateValues` qualifying property shall be incorporated if the signature misses some of the certificates listed in ETSI EN 319 132-1 [1], clause 5.4.1 that are required to validate the XAdES signature. Otherwise it shall not be incorporated into the XAdES signature.

f) Requirement for `RevocationValues`. If a XAdES-E-X-Long signature or a XAdES-E-X-L signature is generated, `RevocationValues` qualifying property shall be incorporated if the signature misses some of the revocation data listed in ETSI EN 319 132-1 [1], clause 5.4.2 that are required to validate the XAdES signature. Otherwise it shall not be incorporated into the XAdES signature.

g) Requirement for `AttrAUthoritiesCertValues`. If a XAdES-E-X-Long signature or a XAdES-E-X-L signature is generated, `AttrAUthoritiesCertValues` qualifying property shall be incorporated if an attribute certificate or a signed assertion has been incorporated in the XAdES signature and some of the certificates required for their validation do not appear in `ds:KeyInfo` or `CertificateValues`. Otherwise it shall not be incorporated into the XAdES signature.

h) Requirement for `AttributeRevocationValues`. If a XAdES-E-X-Long signature or a XAdES-E-X-L signature is generated, `AttributeRevocationValues` qualifying property shall be incorporated if an attribute certificate or a signed assertion has been incorporated in the XAdES signature and some revocation data required for their validation do not appear in `ds:KeyInfo` or `RevocationValues`. Otherwise it shall not be incorporated into the XAdES signature.

i) Requirement for `CertificateValues` and `AttrAuthoritiesCertValues`. Duplication of certificate values within the signature should be avoided.

j) Requirement for `RevocationValues` and `AttributeRevocationValues`. Duplication of revocation values within the signature should be avoided.

NOTE: On `CompleteCertificateRefsV2` and `CompleteRevocationRefs`. In case of direct trust, the `CompleteCertificateRefsV2` and `CompleteRevocationRefs` qualifying properties would not contain any reference, according to the requirements on their contents in ETSI EN 319 132-1 [1], clauses A.1.1 and A.1.1.2 respectively.

A.2 XAdES-E-A signatures built on XAdES-E-C, XAdES-E-X, XAdES-E-X-Long and XAdES-E-X-L signatures

XAdES-E-A signatures may also be built on XAdES-E-C, XAdES-E-X, XAdES-E-X-Long, and XAdES-E-X-L signatures.

XAdES-E-A signatures mentioned in paragraph above are built by adding one or more `ArchiveTimeStamp` qualifying properties defined in namespace whose URI is http://uri.etsi.org/01903/v1.4.1# to XAdES-E-C, XAdES-E-X, XAdES-E-X-Long and XAdES-E-X-L signatures.

Table A.2: Requirements for XAdES-E-A built on XAdES-E-C, XAdES-E-X,
XAdES-E-X-Long and XAdES-E-X-L

Elements/Qualifying properties/Services	Presence in E-A level	Cardinality	Additional notes and requirements	Reference
`SigningTime`	may be present	0 or 1		ETSI EN 319 132-1 [1] clause 5.2.1
`SigningCertificateV2`	conditioned presence	0 or 1	As in table 1	ETSI EN 319 132-1 [1] clause 5.2.2
`CommitmentTypeIndication`	may be present	≥ 0		ETSI EN 319 132-1 [1] clause 5.2.3
`DataObjectFormat`	may be present	≥ 0		ETSI EN 319 132-1 [1] clause 5.2.4
`SignatureProductionPlaceV2`	may be present	0 or 1		ETSI EN 319 132-1 [1] clause 5.2.5
`SignerRoleV2`	may be present	0 or 1		ETSI EN 319 132-1 [1] clause 5.2.6
`CounterSignature`	may be present	≥ 0		ETSI EN 319 132-1 [1] clause 5.2.7.2
`AllDataObjectsTimeStamp`	may be present	≥ 0	As in table 1	ETSI EN 319 132-1 [1], clause 5.2.8.1
`IndividualDataObjectsTimeStamp`	may be present	≥ 0	As in table 1	ETSI EN 319 132-1 [1], clause 5.2.8.2
`SignaturePolicyIdentifier`	may be present	Built on E-EPES: 1 Not built on E-EPES: 0	As in table 1	ETSI EN 319 132-1 [1], clause 5.2.9
`SignaturePolicyStore`	conditioned presence	0 or 1	As in table 1	ETSI EN 319 132-1 [1], clause 5.2.10
`SignatureTimeStamp`	shall be present	≥ 1	As in table 1	ETSI EN 319 132-1 [1], clause 5.3
`CompleteCertificateRefsV2`	shall be present	1	As in table A.1	ETSI EN 319 132-1 [1], clause A.1.1
`AttributeCertificateRefsV2`	conditioned presence	0 or 1	As in table A.1	ETSI EN 319 132-1 [1], clause A.1.3
`CompleteRevocationRefs`	shall be present	1	As in table A.1	ETSI EN 319 132-1 [1], clause A.1.2
`AttributeRevocationRefs`	conditioned presence	0 or 1	As in table A.1	ETSI EN 319 132-1 [1], clause A.1.4
`RefsOnlyTimeStampV2`	may be present	Built on E-X Type 2, E-X-L Type 2: ≥ 1 Built on E-C, E-X Type1, E-X-L Type 1, E-X-Long: ≥ 0	As in table A.1	ETSI EN 319 132-1 [1], clause A.1.5.2
`SigAndRefsTimeStampV2`	may be present	Built on E-X Type 1, E-X-L Type 1: ≥1 Built on E-C, E-X Type 2, E-X-L Type 2, E-X-Long: ≥ 0	As in table A.1	ETSI EN 319 132-1 [1], clause A.1.5.1
`CertificateValues`	conditioned presence	0 or 1	As in table 1	ETSI EN 319 132-1 [1], clause 5.4.1
`RevocationValues`	conditioned presence	0 or 1	As in table 1	ETSI EN 319 132-1 [1], clause 5.4.2
`AttrAuthoritiesCertValues`	conditioned presence	0 or 1	As in table 1	ETSI EN 319 132-1 [1], clause 5.4.3
`AttributeRevocationValues`	conditioned presence	0 or 1	As in table 1	ETSI EN 319 132-1 [1], clause 5.4.4
Service: incorporation of validation data for electronic time-stamps	*	-	As in table 1	ETSI EN 319 132-1 [1], clause 5.5.1
SPO: `TimeStampValidationData`	*	≥ 0	As in table 1	ETSI EN 319 132-1 [1], clause 5.5.1

Elements/Qualifying properties/Services	Presence in E-A level	Cardinality	Additional notes and requirements	Reference
SPO: certificate and revocation values embedded in the electronic time-stamp itself	*	≥ 0	As in table 1	ETSI EN 319 132-1 [1], clause 5.5.1
ArchiveTimeStamp	*	≥ 1	As in table 1	ETSI EN 319 132-1 [1], clause 5.5.2
RenewedDigest	*	≥ 0	As in table 1	ETSI EN 319 132-1 [1], clause 5.5.3

Annex B (informative):
Change History

date	Version	Information about changes
November 2013	V0.0.3	Include an extension mechanism to `xades:SignedSignatureProperties` and `xades:SignedDataObjectProperties`. Restructuring of the document to align with ETSI EN 319 122, addition of new properties: `xadesenv111:SigningCertificate`, `xadesenv111:SignerRole`, `xadesenv111:SignaturePolicyStorage`, `xadesenv111:RenewedDigest`, and `xadesenv111:SPDocSpecification` qualifier and the introduction of different conformance levels.
December 2014	V0.0.6	Changed content to XAdES forms and extensions, as agreed by ESI. Now this part does not contain the Baseline Profile anymore.
January 2015	V0.0.7	Implemented new introduction and scope in line with the strategy agreed by ESI on the scope of the standards. Implemented resolutions to comments to v0.0.6 regarding, among others to terminology (levels instead forms) and legacy signatures. Reviewed requirements for all the levels.
January 2015	V0.0.8	Implemented specifications based on new format of tables as the used in EN 319 132-1.
March 2015	V0.0.10	Implemented resolutions to comments received during public commenting period #2. Final draft for ESI approval.
June 2015	V0.0.11	Approved draft by ETSI ESI.

History

<table>
<tr><th colspan="4">Document history</th></tr>
<tr><td>V1.0.0</td><td>June 2015</td><td>EN Approval Procedure</td><td>AP 20151028: 2015-06-30 to 2015-10-28</td></tr>
<tr><td></td><td></td><td colspan="2"></td></tr>
<tr><td></td><td></td><td colspan="2"></td></tr>
<tr><td></td><td></td><td colspan="2"></td></tr>
<tr><td></td><td></td><td colspan="2"></td></tr>
</table>