ETSI TR 119 112 V1.1.1 (2019-04)

Electronic Signatures and Infrastructures (ESI);
Most significant differences
between AdES/ASiC ENs and previous TSs

Reference
DTR/ESI-0019112

Keywords
ASiC, CAdES, electronic signature, PAdES,
XAdES

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

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables 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 (https://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.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI).

Modal verbs terminology

In the present document "**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.

1 Scope

The present document summarizes:

- The most relevant differences between the CAdES digital signatures specified in ETSI EN 319 122-1 [i.2] and ETSI EN 319 122-2 [i.26], and the CAdES signatures specified in ETSI TS 101 733 (V2.2.1) [i.3] and ETSI TS 103 173 (V2.2.1) [i.4].
- The most relevant differences between the PAdES digital signatures specified in ETSI EN 319 142-1 [i.8] and ETSI EN 319 142-2 [i.9], and the PAdES signatures specified in the latest versions of the different parts ETSI TS 102 778 ([i.10] to [i.15]) and ETSI TS 103 172 (V2.2.2) [i.16].
- The most relevant differences between the XAdES digital signatures specified in ETSI EN 319 132-1 [i.1] and ETSI EN 319 132-2 [i.5], and the XAdES signatures specified in ETSI TS 101 903 (V1.4.2) [i.6] and ETSI TS 103 171 (V2.1.1) [i.7].
- The most relevant differences between the ASiC containers specified in ETSI EN 319 162-1 [i.17] and ETSI EN 319 162-2 [i.18] and the ASiC containers specified in ETSI TS 102 918 (V1.3.1) [i.19] and ETSI TS 103 174 (V2.2.1) [i.20].

2 References

2.1 Normative references

Normative references are not applicable in the present document.

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] ETSI EN 319 132-1 (V1.1.1): "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures".

[i.2] ETSI EN 319 122-1 (V1.1.1): "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures".

[i.3] ETSI TS 101 733 (V2.2.1): "Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)".

[i.4] ETSI TS 103 173 (V2.2.1): "Electronic Signatures and Infrastructures (ESI); CAdES Baseline Profile".

[i.5] ETSI EN 319 132-2 (V1.1.1): "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 2: Extended XAdES signatures".

[i.6] ETSI TS 101 903 (V1.4.2): "Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES)".

[i.7] ETSI TS 103 171 (V2.1.1): "Electronic Signatures and Infrastructures (ESI); XAdES Baseline Profile".

[i.8] ETSI EN 319 142-1 (V1.1.1): "Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures".

[i.9] ETSI EN 319 142-2 (V1.1.1): "Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 2: Additional PAdES signatures profiles".

[i.10] ETSI TS 102 778-1 (V1.1.1): "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 1: PAdES Overview - a framework document for PAdES".

[i.11] ETSI TS 102 778-2 (V1.2.1): "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 2: PAdES Basic - Profile based on ISO 32000-1".

[i.12] ETSI TS 102 778-3 (V1.2.1): "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 3: PAdES Enhanced - PAdES-BES and PAdES-EPES Profiles".

[i.13] ETSI TS 102 778-4 (V1.1.2): "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 4: PAdES Long Term - PAdES LTV Profile".

[i.14] ETSI TS 102 778-5 (V1.1.2): "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 5: PAdES for XML Content - Profiles for XAdES signatures".

[i.15] ETSI TS 102 778-6 (V1.1.1): "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 6: Visual Representations of Electronic Signatures".

[i.16] ETSI TS 103 172 (V2.2.2): "Electronic Signatures and Infrastructures (ESI); PAdES Baseline Profile".

[i.17] ETSI EN 319 162-1 (V1.1.1): "Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 1: Building blocks and ASiC baseline containers".

[i.18] ETSI EN 319 162-2 (V1.1.1): "Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 2: Additional ASiC containers".

[i.19] ETSI TS 102 918 (V1.3.1): "Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC) ".

[i.20] ETSI TS 103 174 (V2.2.1): "Electronic Signatures and Infrastructures (ESI); ASiC Baseline Profile".

[i.21] ISO 32000-1: "Document management - Portable document format - Part 1: PDF 1.7".

[i.22] IETF RFC 4998: "Evidence Record Syntax (ERS)".

[i.23] IETF RFC 6283: "Extensible Markup Language Evidence Record Syntax (XMLERS)".

[i.24] IETF RFC 5652: "Cryptographic Message Syntax (CMS)".

[i.25] IETF RFC 5035 (August 2007): "Enhanced Security Services (ESS) Update: Adding CertID Algorithm Agility".

[i.26] ETSI EN 319 122-2: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 2: Extended CAdES signatures".

[i.27] Commission Implementing Decision (EU) 2015/1506 of 8 September 2015 laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognised by public sector bodies pursuant to Articles 27(5) and 37(5) of 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.

[i.28] W3C Recommendation (11 April 2013): "XML Signature Syntax and Processing Version 1.1".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI EN 319 122-1 [i.2], ETSI EN 319 132-1 [i.1] and ETSI EN 319 162-1 [i.17] apply.

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI EN 319 122-1 [i.2], ETSI EN 319 132-1 [i.1] and ETSI EN 319 162-1 [i.17] apply.

4 Main differences between specifications for CAdES digital signatures

4.1 Introduction

Compared to ETSI TS 101 733 (V2.2.1) [i.3] and ETSI TS 103 173 (V 2.2.1) [i.4], ETSI EN 319 122-1 [i.2] and ETSI EN 319 122-2 [i.26] implemented the following types of differences:

1) Specification of new attributes for them to substitute in the future attributes that had been specified by ETSI TSs.

2) Specification of new attributes, with semantics that the attributes already specified by ETSI TSs did not offer.

3) Clarification of the semantics of certain attributes already specified within the different ETSI TSs whenever ETSI ESI considered worth to implement such clarifications.

4) Deprecation of a number of attributes specified in ETSI TS 101 733 [i.3].

5) Definition of two new sets of signature levels, namely: one set of CAdES baseline signatures, which is specified in ETSI EN 319 122-1 [i.2], and one set of extended CAdES signatures, which is defined in ETSI EN 319 122-2 [i.26]. The first set comes from the revision of the levels defined in ETSI TS 103 173 [i.4]. The second comes from the revision of the levels defined in ETSI TS 101 733 [i.3].

6) Redistribution of material:

    a) ETSI EN 319 122-1 [i.2] contains now: the definition of the semantics and the syntax of the new set of CAdES attributes, and the specification of the CAdES baseline signature levels.

    b) ETSI EN 319 122-2 [i.26].contains the specification of extended CAdES signature levels.

    c) ETSI TS 101 733 [i.3] contained: the definition of the semantics and the syntax of all the previous set of CAdES attributes, and the specification of a set of CAdES signature levels, equivalent to the ones that are specified in ETSI EN 319 122-2 [i.26].

    d) ETSI TS 103 173 [i.4] contained the specification of levels for CAdES baseline signatures old formats.

The following clauses provide further details on some of the aforementioned changes.

4.2 New attributes substituting previously defined ones

Table 8 shows new CAdES attributes specified in ETSI EN 319 122-1 [i.2]. Some of them also replace already existing CAdES attributes specified in ETSI TS 101 733 [i.3], by reasons explained in the table. Others, just allow to incorporate new features into the CAdES signatures.

Table 1: Additional ETSI EN 319 122-1 new qualifying CAdES properties

New CAdES attributes specified in ETSI EN 319 122-1	CAdES attributes specified in ETSI TS 101 733 replaced by the former ones	Reason for replacement OR for their incorporation (if they do not replace none in ETSI TS 101 733)
`signer-attributes-v2`	`signer-attributes`	Add new element able to contain signed assertions. This would be signed by a third party, stronger than claimed assertions but less restrictive than attribute certificates. Add new element able to contain not only X509 attribute certificates but any hypothetical attribute certificate in a different format.
`signature-policy-store`	--	Allow incorporating the full signature policy document, not only its identifier and a pointer to the location where this signature policy document is stored. For self-contained long-lasting signatures in prevision of difficulties to access to the signature policy location.
`ats-hash-index-v3`	`ats-hash-index`	Allow or addition of a value within the set of values in `Attribute.attrValues` field within a certain attribute after the already present values within the aforementioned set had been time-stamped by a former `archive-time-stamp-v3`. This is achieved by computing digests on octets "resulting from concatenating the `Attribute.attrType` field and one of the instances of `AttributeValue` within the `Attribute.attrValues` within the `unsignedAttrs` field". It is worth to mention that `ats-hash-index` attribute is not used in any of the levels that were mentioned in the EU Commission Implementing Decision (EU) 2015/1506 [i.27] (see note).
`SigPolicyQualifierInfo in signature-policy-identifier`	`SigPolicyQualifierInfo in signature-policy-identifier`	A third and new qualifier for the signature policy have been identified so far: an identifier of the technical specification that defines the syntax used for producing the signature policy document (an element of type SPDocSpecification).
NOTE: This attribute is not part of signature formats mentioned in EU commission decision.		

4.3 Clarification of attributes semantics

A relevant effort was put by ESI in clarifying the semantics of a number of attributes. Most of these properties were properties that either contain validation material (certificates, CRLs, OCSP responses) or properties that contain references to this kind of validation material.

Most of the times the clarification consisted in making it clear what specific validation values, or references to what validation values, may be present in each attribute.

It is worth to mention that none of the attributes listed in Table 2 is used in any of the levels that were mentioned in the EU Commission Implementing Decision (EU) 2015/1506 [i.27].

Table 2: Qualifying CAdES properties whose semantics has been clarified

CAdES attributes whose semantics has been clarified	Clauses in ETSI EN 319 122-1
certificate-values	A.1.1.2
revocation-values	A.1.2.2
complete-certificate-references	A.1.1.1
complete-revocation-references	A.1.2.1
attribute-certificate-references	A.1.3
attribute-revocation-references	A.1.4
NOTE: These attributes are not part of signature formats mentioned in EU commission decision.	

In addition to what has been stated above, ETSI EN 319 122-1 [i.2] and ETSI EN 319 122-2 [i.26] clearly specifies that its IssuerSerial component of ESS signing-certificate-v2 attribute is "only a hint, that can help to identify the certificate whose digest matches the value present in the reference. But the binding information is the digest of the certificate", which clearly states that applications cannot not rely on this value for matching a reference to the purportedly referenced certificate; instead, they are required to use the digest value. This was not stated in ETSI TS 101 733 [i.3] and ETSI TS 103 173 [i.4].

4.4 Deprecated attributes

Table 3 shows the attributes deprecated by ETSI EN 319 122-1 [i.2].

Table 3: Attributes deprecated by ETSI EN 319 122-1

other-signing-certificate
signer-attributes
archive-time-stamp (ATSv2)
long-term-validation
ats-hash-index
time-mark
NOTE: These attributes are not part of signature formats mentioned in EU commission decision.

4.5 Two new sets of levels

ETSI EN 319 122-1 [i.2] and ETSI EN 319 122-2 [i.26], being European Standards containing technical specifications targeted at specifying semantics and syntax requirements for technical concepts (digital signatures) that could be used for supporting legal concepts (advanced electronic signatures).

As a direct consequence of this, within ETSI EN 319 122-1 [i.2] and ETSI EN 319 122-2 [i.26], CAdES is not any more an acronym as in ETSI TS 101 733 [i.3] and ETSI TS 103 733 [i.4], but a kind of trademark for shortly naming and identifying a specific type of digital signatures: those ones that are built on CMS signatures as specified in IETF RFC 5652 [i.24], by incorporation of signed and unsigned attributes specified in ETSI EN 319 122-1 [i.2].

Also as a direct consequence of that, ESI decided to differentiate the ETSI EN 319 122-compliant CAdES signatures from the ETSI TS 101 733-compliant or ETSI TS 103 171-compliant CAdES signatures.

ETSI EN 319 122-1 [i.2] and ETSI EN 319 122-2 [i.26] define two sets of levels, most of them replacing levels specified in ETSI TS 103 173 [i.4] and ETSI TS 101 733 [i.3], as indicated in Table 10 and Table 11. It is worth to mention that CAdES-LTA-Level and none of the levels in Table 11 are mentioned in the EU Commission Implementing Decision (EU) 2015/1506 [i.27].

Table 4: Correspondence between levels in ETSI EN 319 122-1 and levels in ETSI TS 103 173 (CAdES baseline signatures)

New levels specified in ETSI EN 319 122-1	Levels in ETSI TS 103 173
CAdES-B-B	CAdES-B-Level
CAdES-B-T	CAdES-T-Level
CAdES-B-LT	CAdES-LT-Level
CAdES-B-LTA	CAdES-LTA-Level
NOTE: These attributes are not part of signature formats mentioned in EU commission decision.	

Table 5: Correspondence between levels in ETSI EN 319 122-2 and levels in ETSI TS 101 733 (extended CAdES signatures)

New levels specified in ETSI EN 319 122-2	Levels in ETSI TS 101 733
CAdES-E-B	CAdES-B
CADES-E-EPES	CADES-EPES
CAdES-E-C	CAdES-C
CAdES-E-X	CAdES-X
CAdES-E-X-Long	CAdES-X-Long
CAdES-E-X-L	CAdES-X-L
CAdES-E-A	CAdES-A

5 Main differences between specifications for XAdES digital signatures

5.1 Introduction

The present document uses the URI namespaces and the prefixes associated to these XML namespaces listed in Table 6.

Table 6: Namespaces with constant prefixes

XML Namespace URI	Prefix
http://www.w3.org/2000/09/xmldsig#	ds
http://uri.etsi.org/01903/v1.3.2#	xades
http://uri.etsi.org/01903/v1.4.1#	xadesv141

Compared to ETSI TS 101 903 (V1.4.2) [i.6] and ETSI TS 103 171 (V2.1.1) [i.7], ETSI EN 319 132-1 [i.1] and ETSI EN 319 132-2 [i.5] implemented the following types of differences:

1) Specification of new qualifying properties for them to substitute in the future qualifying properties that had been specified by ETSI TSs.

2) Specification of new qualifying properties, with semantics that none of the qualifying properties already specified by ETSI TSs did not offer.

3) Clarification of the semantics of certain qualifying properties already specified within the different ETSI TSs whenever ETSI ESI considered worth to implement such clarifications.

4) Definition of two new sets of signature levels, namely: one set of XAdES baseline signatures, which is specified in ETSI EN 319 132-1 [i.1], and one set of extended XAdES signatures, which is defined in ETSI EN 319 132-2 [i.5]. The first set comes from the revision of the levels defined in ETSI TS 103 171 [i.7]. The second comes from the revision of the levels defined in ETSI TS 101 903 [i.6].

5) Redistribution of material:

   a) ETSI EN 319 132-1 [i.1] contains now: the definition of the semantics and the syntax of the new set of XAdES qualifying properties, and the specification of the XAdES baseline signature levels.

b) ETSI EN 319 132-2 [i.5] contains the specification of extended XAdES signature levels.

c) ETSI TS 101 903 [i.6] contained: the definition of the semantics and the syntax of all the previous set of XAdES qualifying properties, and the specification of a set of XAdES signature levels, equivalent to the ones that are specified in ETSI EN 319 132-2 [i.5].

d) ETSI TS 103 171 [i.7] contained the specification of levels for XAdES baseline signatures old formats.

The following clauses will provide further details on some of the aforementioned changes.

5.2 New qualifying properties substituting previously defined ones

The XML Signature W3C Recommendation, which specifies the semantics and syntax of XML signatures, on which XAdES signatures are built, deprecated an element which was used in ETSI TS 101 903 [i.6] and ETSI TS 103 171 [i.7], namely the `ds:X509IssuerSerial` element, due to reported problems by XML validators when dealing with very high integer values. Indeed the problem was not a problem of the specification of such element, but a problem of implementations of certain XML validators.

As it has been mentioned, a number of qualifying properties specified in ETSI TS 101 903 [i.6] contained the aforementioned element.

ESI decided not to keep in its new specifications an element that XML Signature W3C Recommendation had labelled as deprecated. This forced to define new XAdES qualifying properties for substituting:

1) all the previously defined ones containing the `ds:X509IssuerSerial` element; and

2) any previously defined qualifying property whose semantics depended on the properties included in bullet 1).

Table 7 shows the XAdES qualifying properties specified in the ETSI TS 101 903 [i.6] and the new ones specified by ETSI EN 319 132-1 [i.1].

Table 7: ETSI EN 319 132-1 new qualifying XAdES properties replacing ETSI TS 101 903 XAdES qualifying properties due to deprecation of ds:X509IssuerSerial in XML Signature W3C Recommendation

New XAdES qualifying properties specified in ETSI EN 319 132-1	XAdES qualifying properties specified in ETSI TS 101 903 replaced by the former ones
`xades:SigningCertificateV2`	`xades:SigningCertificate`
`xadesv141:CompleteCertificateRefsV2`	`xades:CompleteCertificateRefs`
`xadesv141:AttributeCertificateRefsV2`	`xades:AttributeCertificateRefs`
`xadesv141:SigAndRefsTimeStampV2`	`xades:SigAndRefsTimeStamp`
`xadesv141:RefsOnlyTimeStampV2`	`xades:RefsOnlyTimeStamp`
`xades:SignatureProductionPlaceV2`	`xades:SignatureProductionPlace`

Qualifying properties `xades:SigningCertificate`, `xades:CompleteCertificateRefs`, and `xades:AttributeCertificateRefs` included `ds:X509IssuerSerial` as component.

In these components, the deprecated `ds:X509IssuerSerial` element was replaced by the so-called `xades:IssuerSerialV2` element, which contains the base-64 encoding of one DER-encoded instance of type `IssuerSerial` type defined in IETF RFC 5035 [i.25]. In essence it contains the same information than the `ds:X509IssuerSerial` but in its original encoding within the X509 certificate, which first, keeps the information, and second, avoids any problem appearing by the conversion of a Distinguished Name into a String.

In addition to this ETSI EN 319 132-1 [i.1] clearly specifies that this new element is "only a hint, that can help to identify the certificate whose digest matches the value present in the reference. But the binding information is the digest of the certificate", which clearly states that applications cannot not rely on this value for matching a reference to the purportedly referenced certificate; instead, they are required to use the digest value. This was not stated in ETSI TS 101 903 [i.6] and ETSI TS 103 171 [i.7].

Qualifying properties `xades:SigAndRefsTimeStamp` and `xades:RefsOnlyTimeStamp` depended on some of the properties in the list before.

Table 8 hows new XAdES qualifying properties specified in ETSI EN 319 132-1 [i.1]. Some of them also replace already existing XAdES qualifying properties specified in ETSI TS 101 903 [i.6], by reasons explained in the table. Others, just allow to incorporate new features into the XAdES signatures.

Table 8: Additional ETSI EN 319 132-1 new qualifying XAdES properties

New XAdES qualifying properties specified in ETSI EN 319 132-1	XAdES qualifying properties specified in ETSI TS 101 903 replaced by the former ones	Reason for replacement OR for their incorporation (if they do not replace none in ETSI TS 101 903)
xades:SignatureProductionPlaceV2	xades:SignatureProductionPlace	Add new element for including the street address.
xades:SignerRoleV2	xades:SignerRole	Add new element able to contain signed assertions. This would be signed by a third party, stronger than claimed assertions but less restrictive than attribute certificates. Add new element able to contain not only X509 attribute certificates but any hypothetical attribute certificate in a different format.
xadesv141:SignaturePolicyStore	--	Allow incorporating the full signature policy document, not only its identifier and a pointer to the location where this signature policy document is stored. For self-contained long-lasting signatures in prevision of difficulties to access to the signature policy location.
xadesv141:RenewedDigests	--	For countering the risk of break of digests used in computation of archive time-stamp tokens on signed data objects that are detached of the XAdES signature. This property forces the computation of the digest of such objects with a different algorithm to the one that is suspected to be broken soon.

5.3 Clarification of qualifying properties semantics

A relevant effort was put by ESI in clarifying the semantics of a number of qualifying properties. Most of these properties were properties that either contain validation material (certificates, CRLs, OCSP responses) or properties that contain references to this kind of validation material.

Most of the times the clarification consisted in making it clear what specific validation values, or references to what validation values, may be present in each qualifying property.

Table 9: Qualifying XAdES properties whose semantics has been clarified

XAdES qualifying properties whose semantics has been clarified	Clauses in ETSI EN 319 132-1
xades:CertificateValues	5.4.1
xades:RevocationValues	5.4.2
xades:AttrAuthoritiesCertValues	5.4.3
xades:AttributeRevocationValues	5.4.4
xades:CompleteRevocationRefs	A.1.2
xades:AttributeRevocationRefs	A.1.4

5.4 Two new sets of levels

ETSI EN 319 132-1 [i.1] and ETSI EN 319 132-2 [i.5], being European Standards containing technical specifications targeted at specifying semantics and syntax requirements for technical concepts (digital signatures) that could be used for supporting legal concepts (advanced electronic signatures).

As a direct consequence of this, within ETSI EN 319 132-1 [i.1] and ETSI EN 319 132-2 [i.5], XAdES is not any more an acronym as in ETSI TS 101 903 [i.6] and ETSI TS 103 171 [i.7], but a kind of trademark for shortly naming and identifying a specific type of digital signatures: those ones that are built on XML signatures as specified by W3C XML Signature Recommendation [i.28], by incorporation of signed and unsigned qualifying properties specified in ETSI EN 319 132-1 [i.1].

Also as a direct consequence of that, ESI decided to differentiate the ETSI EN 319 132-compliant XAdES signatures from the ETSI TS 101 903-compliant or ETSI TS 103 171-compliant XAdES signatures.

ETSI EN 319 132-1 [i.1] and ETSI EN 319 132-2[i.5] defines two sets of levels, most of them replacing levels specified in ETSI TS 103 171 [i.7] and ETSI TS 101 903 [i.6], as indicated in Table 10 and Table 11.

Table 10: Correspondence between levels in ETSI EN 319 132-1 and levels in ETSI TS 103 171 (XAdES baseline signatures)

New levels specified in ETSI EN 319 132-1	Levels in ETSI TS 103 171
XAdES-B-B	XAdES-B-Level
XAdES-B-T	XAdES-T-Level
XAdES-B-LT	XAdES-LT-Level
XAdES-B-LTA	XAdES-LTA-Level

Table 11: Correspondence between levels in ETSI EN 319 132-2 and levels in ETSI TS 101 903 (extended XAdES signatures)

New levels specified in ETSI EN 319 132-1	Levels in ETSI TS 103 171
XAdES-E-B	XAdES-B
XADES-E-EPES	XADES-EPES
XAdES-E-C	XAdES-C
XAdES-E-X	XAdES-X
XAdES-E-X-Long	-------
XAdES-E-X-L	XAdES-X-L
XAdES-E-A	XAdES-A

6 Main differences between specifications for PAdES digital signatures

6.1 Introduction

Compared to ETSI TS 102 778 [i.10] to [i.15] and ETSI TS 103 172 (V2.2.2) [i.16], ETSI EN 319 142-1 [i.8] and ETSI EN 319 142-2 [i.9] implemented the following types of differences:

1) Specification of new attributes for them to substitute in the future attributes that had been specified by ETSI TSs.

2) Clarification of the usage and encoding of certain attributes already specified within the different ETSI TSs whenever ETSI ESI considered worth to implement such clarifications.

3) Deprecation of a number of attributes specified in ETSI TS 102 778 [i.10] to [i.15].

4) Definition of two new sets of signature levels, namely: one set of PAdES baseline signatures, which is specified in ETSI EN 319 142-1 [i.8], and one set of extended PAdES signatures, which is defined in ETSI EN 319 142-2 [i.9]. The first set comes from the revision of the levels defined in ETSI TS 103 172 [i.16]. The second comes from the revision of the levels defined in ETSI TS 102 778 [i.10] to [i.15].

5) Redistribution of material:

   a) ETSI EN 319 142-1 [i.8] contains now: the definition of the semantics and the syntax of the new set of PAdES attributes, and the specification of the PAdES baseline signature levels.

b) ETSI EN 319 142-2 [i.9] contains the specification of extended PAdES signature levels.

c) ETSI TS 102 778 [i.11], [i.12], [i.13], [i.14] contained the definition of the semantics and the syntax of all the previous set of PAdES attributes, and the specification of a set of PAdES signature levels, equivalent to the ones that are specified in ETSI EN 319 142-2 [i.9].

d) ETSI TS 103 172 [i.16] contained the specification of levels for PAdES baseline signatures old formats.

e) ETSI TS 102 778-1 [i.10] contained an overview of the set of profiles for PDF Advanced Electronic Signatures specified in the other ETSI TS 102 778 parts [i.11] to [i.15]. Its contents were not included in ETS EN 319 142 [i.8] and [i.9].

f) ETSI TS 102 778-6 [i.15] contained recommendations for the visual representations of advanced electronic signatures (AdES) in PDFs. Its contents were not included in ETSI EN 319 142-1 [i.8] and ETSI EN 319 142-2 [i.9].

The following clauses provide further details on some of the aforementioned changes.

6.2 New attributes substituting previously defined ones

Table 8 shows a new attribute whose usage is specified in ETSI EN 319 142-1 [i.8]. It replaces an already existing CAdES attribute specified in ETSI TS 101 733 [i.3]. It may be present in the DER-encoded SignedData object included as the PDF signature in the entry with the key Contents of the Signature Dictionary, by reasons explained in Table 12.

Table 12: Additional ETSI EN 319 142-1 new qualifying PAdES properties

New PAdES attributes specified in ETSI EN 319 142-1	PAdES attributes specified in ETSI TS 102 778 replaced by the former ones	Reason for replacement OR for their incorporation
`signer-attributes-v2`	`signer-attributes`	Add new element able to contain signed assertions. This would be signed by a third party, stronger than claimed assertions but less restrictive than attribute certificates. Add new element able to contain not only X509 attribute certificates but any hypothetical attribute certificate in a different format.

6.3 Clarification of attributes usage and encoding

A relevant effort was put by ESI in clarifying the usage and encoding of a number of attributes. Most of these properties were properties that either contain information provided by the signer to enable a recipient to identify or contact the signer itself or properties that explain the reason for the signing or properties that contain validation material (certificates, CRLs, OCSP responses).

Most of the times the clarification consisted in making it clear when specific attributes may be present in the PAdES signature.

Table 13: Qualifying PAdES properties whose usage and encoding has been clarified

PAdES attributes whose usage and encoding has been clarified	Clauses in ETSI EN 319 142-1
Filter	6.3
Location	6.3
Name	6.3
ContactInfo	6.3
Reason	6.3
commitment-type-indication	6.3
Certs (DSS Dictionary)	5.4.2.2
OCSPs (DSS Dictionary)	5.4.2.2
CRLs (DSS Dictionary)	5.4.2.2
Cert (VRI Dictionary)	5.4.2.3
CRL (VRI Dictionary)	5.4.2.3
OCSP (VRI Dictionary)	5.4.2.3

6.4 Deprecated attributes

Table 14 shows the attributes deprecated by ETSI EN 319 142-1 [i.8].

Table 14: Attributes deprecated by ETSI EN 319 142-1

signer-attributes
time-mark

6.5 Two new sets of levels

ETSI EN 319 142-1 [i.8] and ETSI EN 319 142-2 [i.9], being European Standards containing technical specifications targeted at specifying semantics and syntax requirements for technical concepts (digital signatures) that could be used for supporting legal concepts (advanced electronic signatures).

As a direct consequence of this, within ETSI EN 319 142-1 [i.8] and ETSI EN 319 142-2 [i.9], PAdES is not any more an acronym as in ETSI TS 102 778 [i.11], [i.12], [i.13], [i.14] and ETSI TS 103 172 [i.16], but a kind of trademark for shortly naming and identifying a specific type of digital signatures: those ones built on PDF signatures specified in ISO 32000-1 [i.21] with an alternative signature encoding to support digital signature formats equivalent to the signature format CAdES as specified in ETSI EN 319 122-1 [i.2], by incorporation of signed and unsigned attributes, which fulfil certain common requirements (such as the long term validity of digital signatures) in a number of use cases.

Also as a direct consequence of that, ESI decided to differentiate the ETSI EN 319 142-compliant PAdES signatures from the ETSI TS 102 778-compliant or ETSI TS 103 172-compliant PAdES signatures.

ETSI EN 319 142-1 [i.8] and ETSI EN 319 142-2 [i.9] defines two sets of levels, most of them replacing levels specified in ETSI TS 103 172 [i.16] and ETSI TS 102 778 [i.10] to [i.15], as indicated in Tables 15 and Table 16. It is worth to mention that PAdES-LTA-Level and none of the levels in Table 16 are mentioned in the EU Commission Implementing Decision (EU) 2015/1506 [i.27].

Table 15: Correspondence between levels in ETSI EN 319 142-1 and levels in ETSI TS 103 172 (PAdES baseline signatures)

New levels specified in ETSI EN 319 122-1	Levels in ETSI TS 103 173
PAdES-B-B	PAdES-B-Level
PAdES-B-T	PAdES-T-Level
PAdES-B-LT	PAdES-LT-Level
PAdES-B-LTA	PAdES-LTA-Level

Table 16: Correspondence between levels in ETSI EN 319 142-2 and levels in ETSI TS 102 778 (extended PAdES signatures)

New levels specified in ETSI EN 319 142-2	Levels in ETSI TS 102 778
CMS Signatures in PDF	PAdES Basic
PAdES-E-BES	PAdES-BES
PADES-E-EPES	PADES-EPES
PAdES-E-LTV	PAdES-LTV

7 Main differences between specifications for ASIC containers

7.1 Introduction

Compared to ETSI TS 102 918 (V1.3.1) [i.19] and ETSI TS 103 174 (V2.1.1) [i.20], ETSI EN 319 162-1 [i.17] and ETSI EN 319 162-2 [i.18] implemented the following types of differences:

1) Updated reference to ETSI EN 319 122-1 [i.2] and ETSI EN 319 122-2 [i.26] instead of ETSI TS 101 733 (V2.2.1) [i.3] and ETSI TS 103 173 (V2.2.1) [i.4] for ASiC containers based on CAdES. See clause 5 of the present document for specific information about differences related to CAdES standards.

2) Updated reference to ETSI EN 319 132-1 [i.1] and ETSI EN 319 132-2 [i.5] instead of ETSI TS 101 903 (V1.4.2) [i.6] and ETSI TS 103 171 (V2.2.1) [i.7] for ASiC containers based on XAdES. See clause 6 of the present document for specific information about differences related to XAdES standards.

3) Definition of two new sets of container levels, namely: one set of ASiC baseline containers, which is specified in ETSI EN 319 162-1 [i.17], and one set of Additional ASiC containers, which is defined in ETSI EN 319 162-2 [i.18]. The first set comes from the revision of a subset of levels defined in ETSI TS 103 174 [i.20].

4) Reduction of the number of baseline container types from 6 specified in ETSI TS 103 174 [i.20] to 3 specified in ETSI EN 319 162-1 [i.17]; the 3 types that are not among the baseline profiles have been added to ETSI EN 319 162-2 [i.18] as additional profiles.

5) Support of IETF RFC 4998 [i.22] and IETF RFC 6283 [i.23] evidence records in ETSI EN 319 162-1 [i.17] building blocks and ETSI EN 319 162-2 [i.18] additional ASiC containers.

6) Introduction of new specific Manifest files for long term availability for containers types where this feature cannot be achieved with direct use of signature or time assertion formats attributes/qualifying properties.

7) Clarification of text to eliminate ambiguities.

7.2 Two new sets of container levels

ETSI EN 319 162-1 [i.17] and ETSI EN 319 162-2 [i.18] defines two sets of levels, most of them replacing levels specified in ETSI TS 103 174 [i.20] and ETSI TS 102 918 [i.19], as indicated in Tables 17 and 18. It is worth to mention that ETSI TS 103 174 [i.20] is refenced by the EU Commission Implementing Decision (EU) 2015/1506 [i.27].

Table 17: Correspondence between levels in ETSI EN 319 162-1 and levels in ETSI TS 103 174 (ASiC baseline profiles as baseline containers)

New levels specified in ETSI EN 319 162-1	Levels in ETSI TS 103 174
ASiC-S with CAdES B-B level	ASiC-S with CAdES B-Level
ASiC-S with XAdES B-B level	ASiC-S with XAdES B-Level
ASiC-E with XAdES B-B level	ASiC-E with XAdES B-Level
ASiC-S with CAdES B-T level	ASiC-S with CAdES T-Level
ASiC-S with XAdES B-T level	ASiC-S with XAdES T-Level
ASiC-E with XAdES B-T level	ASiC-E with XAdES T-Level
ASiC-S with CAdES B-LT level	ASiC-S with CAdES LT-Level
ASiC-S with XAdES B-LT level	ASiC-S with XAdES LT-Level
ASiC-E with XAdES B-LT level	ASiC-E with XAdES LT-Level
ASiC-S with CAdES B-LTA level	ASiC-S with CAdES LTA-Level
ASiC-S with XAdES B-LTA level	ASiC-S with XAdES LTA-Level
ASiC-E with XAdES B-LTA level	ASiC-E with XAdES LTA-Level

Table 18: Correspondence between levels in ETSI EN 319 162-2 and levels in ETSI TS 103 174 (ASiC baseline profiles as additional containers)

New levels specified in ETSI EN 319 162-2	Levels in ETSI TS 102 918
ASiC-S Time assertion	ASiC-S Time stamp token
ASiC-E CAdES	ASiC-E XAdES (B/T/LT Level)
ASiC-E Time Assertion	ASiC-E Time stamp token

7.3 Evidence records

ETSI EN 319 162-1 [i.17] building blocks uses the term "Time Assertion" to encompass both time stamp tokens and evidence records as specified in IETF RFC 4998 [i.22] and IETF RFC 6283 [i.23].

Evidence records are also supported in ASiC manifest files allowing to specify the data object(s) to which the evidence records apply.

ETSI EN 319 162-2 [i.18] additional ASiC containers extends to evidence records the baseline profiles with time stamp tokens listed in Table 18.

7.4 New ASiC Manifest files for long term availability

ASiCArchiveManifest was added to protect long term time stamp tokens and ASiCEvidenceRecordManifest was added to reference a set of files to which an evidence record applies, allowing an LTA equivalent level also for ASiC containers with time assertions.

History

Document history		
V1.1.1	April 2019	Publication