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

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 prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

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
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

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

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].