Draft ETSI EN 319 122-2 V1.0.0 (2015-06)

EUROPEAN STANDARD

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

Reference

DEN/ESI-0019122-2

Keywords

ASN.1, CAdES, electronic signature, security

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

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 CAdES digital signatures. Full details of the entire series can be found in part 1 [1].

The present document partly contains an evolved specification of CAdES previously published as ETSI TS 101 733 [i.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.7].

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.2]). See ETSI TR 119 100 [i.4] for getting guidance on how to use the present document within the aforementioned framework.

1 Scope

The present document specifies CAdES digital signatures. CAdES signatures are built on CMS signatures [i.8], by incorporation of signed and unsigned attributes, 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 CAdES 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 CAdES extended signatures a higher degree of optionality than the CAdES baseline signatures specified in ETSI EN 319 122-1 [1].

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

NOTE: Specifically but not exclusively, CAdES 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.7].

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 reference 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 319 122-1: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES 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 reference 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 TS 101 733: "Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)".

[i.2] ETSI TR 119 000: "Electronic Signatures and Infrastructures (ESI); Rationalized structure for Electronic Signature Standardization".

[i.3] ETSI TR 119 001: "Electronic Signatures and Infrastructures (ESI); Definitions and abbreviations".

[i.4] ETSI TR 119 100: "Electronic Signatures and Infrastructures (ESI); Business Driven Guidance for Signature Creation and Validation".

[i.5] ETSI TS 119 172-1: "Electronic Signatures and Infrastructures (ESI); Signature policies; Part 1: Building blocks and table of contents for human readable signature policy documents".

[i.6] ETSI TS 119 312: "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites".

[i.7] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[i.8] IETF RFC 5652 (2009): "Cryptographic Message Syntax (CMS)".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in ETSI TR 119 001 [i.3] and the following apply:

CAdES signature: digital signature that satisfies the requirements specified within the present document

digital signature: data appended to, or a cryptographic transformation (see cryptography) of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient

legacy CAdES 101 733 signature: CAdES signature generated according to ETSI TS 101 733 [i.1]

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI TR 119 001 [i.3] apply.

4 Additional CAdES levels without references to validation data

4.1 Overview

The present document specifies a number of additional levels of CAdES.

Each level is created by a combination of attributes defined in ETSI EN 319 122-1 [1].

NOTE 1: Clause 4.3 defines four CAdES levels namely the CAdES-E-BES, CAdES-E-EPES, CAdES-E-T, and CAdES-E-A built on CAdES-E-T. The normative annex A defines levels of CAdES signatures incorporating attributes that encapsulate references to validation data and attributes that encapsulate time-stamp tokens on the aforementioned references.

NOTE 2: The requirements on the presence and cardinality of the attributes for each CAdES signature level are expressed in tables whose formats and semantics are as specified in clause 6.2.2 of ETSI EN 319 122-1 [1].

4.2 General requirements

The general CMS syntax shall be as specified in ETSI EN 319 122-1 [1], clause 4.

The signature shall contain a CMS `SignedData`, as defined in ETSI EN 319 122-1 [1], clause 4.4 and at least one `SignerInfo` (ETSI EN 319 122-1 [1], clauses 4.6).

The algorithms and key lengths used to generate signatures should comply with ETSI TS 119 312 [i.6].

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

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

CAdES-E-EPES signatures are built on CAdES-E-BES signatures by adding one `signature-policy-identifier` attribute.

CAdES-E-T signatures are built on CAdES-E-BES or CAdES-E-EPES signatures by adding one or more `signature-time-stamp` attributes.

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

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

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

Signature fields/Attributes/Services	Presence in E-BES level	Presence in E-EPES level	Presence in E-T level	Presence in E-A level	Cardinality	References	Additional requirements and notes
content-type	shall be present	shall be present	shall be present	shall be present	1	ETSI EN 319 122-1 [1], clause 5.1.1	
message-digest	shall be present	shall be present	shall be present	shall be present	1	ETSI EN 319 122-1 [1], clause 5.1.2	
Service: protection of signing certificate	shall be provided	shall be provided	shall be provided	shall be provided	1	ETSI EN 319 122-1 [1], clause 5.2.2	
SPO: ESS signing-certificate	conditioned presence	conditioned presence	conditioned presence	conditioned presence	0 or 1	ETSI EN 319 122-1 [1], clause 5.2.2.2	a, e
SPO: ESS signing-certificate-v2	conditioned presence	conditioned presence	conditioned presence	conditioned presence	0 or 1	ETSI EN 319 122-1 [1], clause 5.2.2.3	b, e
Signing-time	may be present	may be present	may be present	may be present	0 or 1	ETSI EN 319 122-1 [1], clause 5.2.1	
commitment-type-indication	may be present	may be present	may be present	may be present	0 or 1	ETSI EN 319 122-1 [1], clause 5.2.3	
content-hints	may be present	may be present	may be present	may be present	0 or 1	ETSI EN 319 122-1 [1], clause 5.2.4.1	
mime-type	may be present	may be present	may be present	may be present	0 or 1	ETSI EN 319 122-1 [1], clause 5.2.4.2	
signer-location	may be present	may be present	may be present	may be present	0 or 1	ETSI EN 319 122-1 [1], clause 5.2.5	
signer-attributes-v2	may be present	may be present	may be present	may be present	0 or 1	ETSI EN 319 122-1 [1], clause 5.2.6.1	
countersignature	may be present	may be present	may be present	may be present	≥ 0	ETSI EN 319 122-1 [1], clause 5.2.7	
content-time-stamp	may be present	may be present	may be present	may be present	≥ 0	ETSI EN 319 122-1 [1], clause 5.2.8	1
signature-policy-identifier	*	shall be present	may be present	may be present	E-EPES: 1 E-BES, E-T, E-A: 0 or 1	ETSI EN 319 122-1 [1], clause 5.2.9.1	2, 3
signature-policy-store	*	conditioned presence	conditioned presence	conditioned presence	0 or 1	ETSI EN 319 122-1 [1], clause 5.2.10	c
content-reference	may be present	may be present	may be present	may be present	0 or 1	ETSI EN 319 122-1 [1], clause 5.2.11	
content-identifier	may be present	may be present	may be present	may be present	0 or 1	ETSI EN 319 122-1 [1], clause 5.2.12	
signature-time-stamp	*	*	shall be present	shall be present	E-BES, E-EPES: ≥ 0 E-T, E-A: ≥ 1	ETSI EN 319 122-1 [1], clause 5.3	f, 1, 4
complete-certificate-references	*	*	*	*	0 or 1	ETSI EN 319 122-1 [1], clause A.1.1.1	e

Signature fields/Attributes/Services	Presence in E-BES level	Presence in E-EPES level	Presence in E-T level	Presence in E-A level	Cardinality	References	Additional requirements and notes
`complete-revocation-references`	*	*	*	*	0 or 1	ETSI EN 319 122-1 [1], clause A.1.2.1	
`attribute-certificate-references`	*	*	*	*	0 or 1	ETSI EN 319 122-1 [1], clause A.1.3	d, e
`attribute-revocation-references`	*	*	*	*	0 or 1	ETSI EN 319 122-1 [1], clause A.1.4	d
`CAdES-C-timestamp`	*	*	*	*	≥ 0	ETSI EN 319 122-1 [1], clause A.1.5.2	1
`time-stamped-certs-crls-references`	*	*	*	*	≥ 0	ETSI EN 319 122-1 [1], clause A.1.5.1	1
Service: certificate values in long-term validation	*	*	*	shall be provided	E-BES, E-EPES, E-T: ≥ 0 E-A: ≥ 1		g, h
SPO: `SignedData.certificates`	*	*	*	conditioned presence	0 or 1	ETSI EN 319 122-1 [1], clause 4.4	i
SPO: `certificate-values`	*	*	*	*	0 or 1	ETSI EN 319 122-1 [1], clause A.1.1.2	
Service: revocation values in long-term validation	*	*	*	shall be provided	E-BES, E-EPES, E-T: 0 or 1 E-A: 1		j,k
SPO: `SignedData.crls.crl`	*	*	*	conditioned presence	0 or 1	ETSI EN 319 122-1 [1], clause 4.4	l
SPO: `SignedData.crls.other`	*	*	*	conditioned presence	0 or 1	ETSI EN 319 122-1 [1], clause 4.4	m
SPO `revocation-values`	*	*	*	*	0 or 1	ETSI EN 319 122-1 [1], clause A.1.2.2	
Service: add archive time-stamp	*	*	*	shall be provided	E-BES, E-EPES, E-T: ≥ 0 E-A: ≥ 1	ETSI EN 319 122-1 [1], clause 5.6.1	
SPO: `archive-time-stamp-v3`	*	*	*	conditioned presence	≥ 0	ETSI EN 319 122-1 [1], clause 5.6.2	n, o, p
SPO: `long-term-validation`	*	*	*	conditioned presence	≥ 0	ETSI EN 319 122-1 [1], clause A.2.5	n, o, q, 5

Additional requirements:

a) Requirement for SPO: ESS `signing-certificate`. The ESS `signing-certificate` attribute shall be used if the SHA-1 hash algorithm is used.

b) Requirement for SPO: ESS `signing-certificate-`v2. The ESS `signing-certificate-v2` attribute shall be used when another hash algorithms than SHA-1 is used.

c) Requirement for `signature-policy-store`. The `signature-policy-store` attribute may be incorporated in the CAdES signature only if the `signature-policy-identifier` attribute is also incorporated and it contains in `sigPolicyHash the` digest value of the signature policy document, Otherwise the `signature-policy-store` shall not be incorporated in the CAdES signature.

d) Requirement for `attribute-certificate-references`.The `attribute-certificate-references` and `attribute-revocation-references` attributes may be used when a at least a certified signer attribute (`certifiedAttributesV2` as defined in clause 5.2.6.1 of ETSI EN 319 122-1 [1]) or a signed assertion (`signedAssertsions` as defined in clause 5.2.6.1 of ETSI EN 319 122-1 [1]) is present within the signer attributes in the digital signature. Otherwise, `attribute-certificate-references` and `attribute-revocation-references` attributes shall not be used.

e) Requirement for SPO: ESS `signing-certificate`, SPO: ESS `signing-certificate-v2`, `complete-certificate-references`, and `attribute-certificate-references`. The `issuerSerial` field should not be included in the encoding of the `ESSCertID`, `ESSCertIDv2` or `OtherCertID` type.

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

g) Requirement for Service: certificate values in long-term validation. The generator shall include the full set of certificates, including the trust anchors when they are available in the form of certificates that have been used to validate the signature. This set includes certificates required for validating the signing certificate, for validating any attribute certificate present in the signature, for validating revocation information (i.e. OCSP response and CRL) if certificates are not already included, and for validating any time-stamp token's signing certificate (i.e. a TSA certificate) already incorporated to the signature.

h) Requirement for Service: certificate values in long-term validation. Duplication of certificate values within the signature should be avoided.

i) Requirement for SPO: `SignedData.certificates`. If the certificate values in the long-term validation are not yet included elsewhere in the signature, they shall be included in `SignedData.certificate`, following the requirements in clause 5.5.3 of ETSI EN 319 122-1 [1].

j) Requirement for Service: revocation values in long-term validation. The generator shall include the full set of revocation data (CRL or OCSP responses) that have been used in the validation of the signature. This set includes all certificate status information required for validating the signing certificate, for validating any attribute certificate or signed assertion present in the signature, for validating revocation information (i.e. OCSP response and CRL) if they are not already included and for validating any time-stamp token's signing certificate (i.e. a TSA certificate) already incorporated to the signature.

k) Requirement for Service: revocation values in long-term validation. Duplication of revocation values within the signature should be avoided.

l) Requirement for SPO: `SignedData.crls.crl`. When the full set of revocation data contains CRLs and this information is not yet included otherwise in the signature, then the CRL values shall be included within `SignedData.crls.crl`.

m) Requirement for SPO: `SignedData.crls.other`. When the full set of revocation data contains OCSP responses and this information is not yet included otherwise in the signature, then the OCSP response values shall be included within `SignedData.crls.other`.

n) Requirement for SPO: `archive-time-stamp-v3` and SPO: `long-term-validation`. When a `long-term-validation` attribute is not present, applications shall generate an `archive-time-stamp-v3` attribute whenever a new archive time-stamp is needed.

o) Requirement for SPO: `archive-time-stamp-v3` and SPO: `long-term-validation`.When a `long-term-validation` attribute is already present, applications shall generate a `long-term-validation` attribute whenever the archive time-stamp needs renewal.

p) Requirement for SPO: `archive-time-stamp-v3`. Before generating and incorporating an `archive-time-stamp-v3` attribute, all the validation material required for verifying the signature, which are not already in the signature, shall be included. This validation material includes validation material used to validate previous archive time stamp.

q) Requirement for SPO: `long-term-validation`. Before adding an additional `long-term-validation` attributes, all the validation material required for verifying the signature and previous `long-term-validation` attributes, which are not already in the signature, shall be included in the fields `extraCertificates` and `extraRevocation` of the new `long-term-validation` attribute.

NOTE 1: On `content-time-stamp`, `signature-time-stamp`, `CAdES-C-timestamp`, and `time-stamped-certs-crls-references`. Several instances of this attribute can occur in the digital signature, from different TSUs.

NOTE 2: On `signature-policy-identifier`. The signature policy can establish specific requirements for other attributes.

NOTE 3: On `signature-policy-identifier`. Further information on signature policies is provided in ETSI TS 119 172-1 [i.5].

NOTE 4: On `signature-time-stamp`. Trusted time indications provides the initial steps towards providing long-term validity.

NOTE 5: On SPO: `long-term-validation`. This form of electronic signature also provides protection against a TSP key compromise.

5 Legacy signatures

When new attributes are incorporated to legacy CAdES 101 733 signatures, these attributes shall comply with ETSI EN 319 122-1 [1].

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

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

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

CAdES-E-X signatures are built on CAdES-E-C signatures by adding one or more time-stamp container properties.

CAdES-E-X type 1 signatures are built on CAdES-E-C signatures by adding one or more `CAdES-C-Timestamp attributes` each.

CAdES-E-X type 2 signatures are built on CAdES-E-C signatures by adding one or more `time-stamped-certs-crls-references attributes` each.

CAdES-E-X-Long signatures are built on CAdES-E-C signature by adding attributes that contain certificates and revocation values.

CAdES-E-X-L Type 1 signatures are built on CAdES-E-X Type 1 signatures by adding attributes that contain certificates and revocation values.

CAdES-E-X-L Type 2 signatures are built on CAdES-E-X Type 2 signatures by adding attributes that contain certificates and revocation values.

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

Signature fields/Attributes/ Services	Presence in E-C level	Presence in E-X level	Presence in E-X-Long level	Presence in E-X-L level	Cardinality	References	Additional requirements and notes
content-type	shall be present	shall be present	shall be present	shall be present	1	ETSI EN 319 122-1 [1], clause 5.1.1	
message-digest	shall be present	shall be present	shall be present	shall be present	1	ETSI EN 319 122-1 [1], clause 5.1.2	
Service: protection of signing certificate	shall be provided	shall be provided	shall be provided	shall be provided	1	ETSI EN 319 122-1 [1], clause 5.2.2	
SPO: ESS signing-certificate	conditioned presence	conditioned presence	conditioned presence	conditioned presence	0 or 1	ETSI EN 319 122-1 [1], clause 5.2.2.2	as in Table 1
SPO: ESS signing-certificate-v2	conditioned presence	conditioned presence	conditioned presence	conditioned presence	0 or 1	ETSI EN 319 122-1 [1], clause 5.2.2.3	as in Table 1
Signing-time	may be present	may be present	may be present	may be present	0 or 1	ETSI EN 319 122-1 [1], clause 5.2.1	
commitment-type-indication	may be present	may be present	may be present	may be present	0 or 1	ETSI EN 319 122-1 [1], clause 5.2.3	
content-hints	may be present	may be present	may be present	may be present	0 or 1	ETSI EN 319 122-1 [1], clause 5.2.4.1	
mime-type	may be present	may be present	may be present	may be present	0 or 1	ETSI EN 319 122-1 [1], clause 5.2.4.2	
signer-location	may be present	may be present	may be present	may be present	0 or 1	ETSI EN 319 122-1 [1], clause 5.2.5	
signer-attributes-v2	may be present	may be present	may be present	may be present	0 or 1	ETSI EN 319 122-1 [1], clause 5.2.6.1	
countersignature	may be present	may be present	may be present	may be present	≥ 0	ETSI EN 319 122-1 [1], clause 5.2.7	
content-time-stamp	may be present	may be present	may be present	may be present	≥ 0	ETSI EN 319 122-1 [1], clause 5.2.8	as in Table 1
signature-policy-identifier	may be present	may be present	may be present	may be present	0 or 1	ETSI EN 319 122-1 [1], clause 5.3.9	as in Table 1
signature-policy-store	conditioned presence	conditioned presence	conditioned presence	conditioned presence	0 or 1	ETSI EN 319 122-1 [1], clause 5.2.10	as in Table 1
content-reference	may be present	may be present	may be present	may be present	0 or 1	ETSI EN 319 122-1 [1], clause 5.2.11	
content-identifier	may be present	may be present	may be present	may be present	0 or 1	ETSI EN 319 122-1 [1], clause 5.2.12	
signature-time-stamp	shall be present	shall be present	shall be present	shall be present	≥ 1	ETSI EN 319 122-1 [1], clause 5.3	as in Table 1
complete-certificate-references	shall be present	shall be present	shall be present	shall be present	1	ETSI EN 319 122-1 [1], clause A 1.1.1	a, 1, 2, 3
complete-revocation-references	shall be present	shall be present	shall be present	shall be present	1	ETSI EN 319 122-1 [1], clause A.1.2.1	a, 1, 2, 3

Signature fields/Attributes/ Services	Presence in E-C level	Presence in E-X level	Presence in E-X-Long level	Presence in E-X-L level	Cardinality	References	Additional requirements and notes
`attribute-certificate-references`	conditioned presence	conditioned presence	conditioned presence	conditioned presence	0 or 1	ETSI EN 319 122-1 [1], clause A.1.3	a, b, 1, 2, 3
`attribute-revocation-references`	conditioned presence	conditioned presence	conditioned presence	conditioned presence	0 or 1	ETSI EN 319 122-1 [1], clause A.1.4	a, b, 1, 2, 3
`CAdES-C-timestamp`	*	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	ETSI EN 319 122-1 [1], clause A.1.5.2	as in Table 1
`time-stamped-certs-crls-references`	*	shall be present in E-X Type 2	*	shall be present in E-X-L Type 1	E-C, E-X-Long, E-X Type 1, E-X-L Type 1: ≥ 0 E-X Type 2, E-X-L Type 2: ≥ 1	ETSI EN 319 122-1 [1], clause A.1.5.1	as in Table 1
Service: certificate values in long-term validation	*	*	shall be provided	shall be provided	E-C, E-X: 0 or 1 E-X-Long, E-X-L: 1		as in Table 1
SPO: `SignedData.certificates`	may be present	may be present	may be present	may be present	0 or 1	ETSI EN 319 122-1 [1], clause 4.4	
SPO: `certificate-values`	*	*	shall be present	shall be present	E-C, E-X: 0 or 1 E-X-Long, E-X-L: 1	ETSI EN 319 122-1 [1], clause A.1.1.2	c
Service: revocation values in long-term validation	*	*	shall be provided	shall be provided	E-C, E-X: 0 or 1 E-X-Long, E-X-L: 1		as in Table 1
SPO: `SignedData.crls.crl`	may be present	may be present	may be present	may be present	0 or 1	ETSI EN 319 122-1 [1], clause 4.4	
SPO: `SignedData.crls.other`	may be present	may be present	may be present	may be present	0 or 1	ETSI EN 319 122-1 [1], clause 4.4	

Signature fields/Attributes/ Services	Presence in E-C level	Presence in E-X level	Presence in E-X-Long level	Presence in E-X-L level	Cardinality	References	Additional requirements and notes
SPO: `revocation-values`	*	*	shall be present	shall be present	E-C, E-X: 0 or 1 E-X-Long, E-X-L: 1	ETSI EN 319 122-1 [1], clause A.1.2.2	d
Service: add archive time-stamp	*	*	*	*	≥ 0	ETSI EN 319 122-1 [1], clause 5.6.1	
SPO: `archive-time-stamp-v3`	*	*	*	*	≥ 0	ETSI EN 319 122-1 [1], clause 5.6.2	
SPO: `long-term-validation`	*	*	*	*	≥ 0	ETSI EN 319 122-1 [1], clause A.2.5	

Additional requirements:

a) Requirement for complete-certificate-references, complete-revocation-references, attribute-certificate-references, and attribute-revocation-references. In case of direct trust, i.e. when the signing certificate contains the trust anchor public key, CAdES-E-C signatures and any signature built on it (i.e. CAdES-E-X Type 1, CAdES-E-X Type 2, CAdES-E-X-L, CAdES-E-X-L Type 1, and CAdES-E-X-L Type 2 signatures) shall not be generated. See note 1 for rationale.

b) Requirement on attribute-certificate-references and attribute-revocation-references. The attributes shall be present if a at least a certified signer attribute (certifiedAttributesV2 as defined in clause 5.2.6.1 of ETSI EN 319 122-1 [1]) or a signed assertion (signedAssertsions as defined in clause 5.2.6.1 of ETSI EN 319 122-1 [1]) is present within the signer attributes in the electronic signature.

c) Requirement on SPO: certificate-values. The certificates shall be added as defined in ETSI EN 319 122-1 [1], clause A.1.1.2.

d) Requirement on SPO: revocation-values. The validation data shall be added as defined in ETSI EN 319 122-1 [1], clause A.1.2.2.

NOTE 1: On complete-certificate-references, complete-revocation-references, attribute-certificate-references, and attribute-revocation-references. In case of direct trust, the complete-certificate-references and the complete-revocation-references attributes would not contain any reference according to the requirements on their contents.

NOTE 2: On complete-certificate-references, complete-revocation-references, attribute-certificate-references, and attribute-revocation-references. If the signer provides as a minimum the CAdES-E-BES or CAdES-E-EPES, then as long as the signature is still valid it can be extended to CAdES-E-C.

NOTE 3: On complete-certificate-references, complete-revocation-references, attribute-certificate-references, and attribute-revocation-references. Time-stamp tokens can themselves include unsigned attributes required to validate the time-stamp token.

A.2 CAdES-E-A signatures on CAdES signatures with references to validation data

CAdES-E-A signatures may also be built on CAdES-E-C, CAdES-E-X, CAdES-E-X-Long, and CAdES-E-X-L signatures as defined in Table A.2.

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

Signature fields/Attributes/Services	Presence in E-A level	Cardinality	References	Additional requirements and notes
content-type	shall be present	1	ETSI EN 319 122-1 [1], clause 5.1.1	
message-digest	shall be present	1	ETSI EN 319 122-1 [1], clause 5.1.2	
Service: protection of signing certificate	shall be provided	1	ETSI EN 319 122-1 [1], clause 5.2.2	
SPO: ESS signing-certificate	conditioned presence	0 or 1	ETSI EN 319 122-1 [1], clause 5.2.2.2	as in Table 1
SPO: ESS signing-certificate-v2	conditioned presence	0 or 1	ETSI EN 319 122-1 [1], clause 5.2.2.3	as in Table 1
Signing-time	may be present	0 or 1	ETSI EN 319 122-1 [1], clause 5.2.1	
commitment-type-indication	may be present	0 or 1	ETSI EN 319 122-1 [1], clause 5.2.3	

Signature fields/Attributes/Services	Presence in E-A level	Cardinality	References	Additional requirements and notes
`content-hints`	may be present	0 or 1	ETSI EN 319 122-1 [1], clause 5.2.4.1	
`mime-type`	may be present	0 or 1	ETSI EN 319 122-1 [1], clause 5.2.4.2	
`signer-location`	may be present	0 or 1	ETSI EN 319 122-1 [1], clause 5.2.5	
`signer-attributes-v2`	may be present	0 or 1	ETSI EN 319 122-1 [1], clause 5.2.6.1	
`countersignature`	may be present	≥ 0	ETSI EN 319 122-1 [1], clause 5.2.7	
`content-time-stamp`	may be present	≥ 0	ETSI EN 319 122-1 [1], clause 5.2.8	as in Table 1
`signature-policy-identifier`	may be present	0 or 1	ETSI EN 319 122-1 [1], clause 5.2.9.1	as in Table 1
`signature-policy-store`	conditioned presence	0 or 1	ETSI EN 319 122-1 [1], clause 5.2.10	as in Table 1
`content-reference`	may be present	0 or 1	ETSI EN 319 122-1 [1], clause 5.2.11	
`content-identifier`	may be present	0 or 1	ETSI EN 319 122-1 [1], clause 5.2.12	
`signature-time-stamp`	shall be present	≥ 1	ETSI EN 319 122-1 [1], clause 5.3	as in Table 1
`complete-certificate-references`	shall be present	0 or 1	ETSI EN 319 122-1 [1], clause A.1.1.1	as in Table A.1
`complete-revocation-references`	shall be present	0 or 1	ETSI EN 319 122-1 [1], clause A.1.2.1	as in Table A.1
`attribute-certificate-references`	conditioned presence	0 or 1	ETSI EN 319 122-1 [1], clause A.1.3	as in Table A.1
`attribute-revocation-references`	conditioned presence	0 or 1	ETSI EN 319 122-1 [1], clause A.1.4	as in Table A.1
`CAdES-C-timestamp`	may be present	Build on E-C, E-X-Long, E-X Type 2, E-X-L Type 2: ≥ 0 Build on E-X Type 1, E-X-L Type 1: ≥ 1	ETSI EN 319 122-1 [1], clause A.1.5.2	as in Table 1
`time-stamped-certs-crls-references`	may be present	Build on E-C, E-X-Long, E-X Type 1, E-X-L Type 1: ≥ 0 Build on E-X Type 2, E-X-L Type 2: ≥ 1	ETSI EN 319 122-1 [1], clause A.1.5.1	as in Table 1
Service: certificate values in long-term validation	shall be provided	1		as in Table 1
SPO: `SignedData.certificates`	conditioned presence	1	ETSI EN 319 122-1 [1], clause 4.4	as in Table 1
SPO: `certificate-values`	may be present	Build on E-C, E-X: 0 or 1 Build on E-X-Long, E-X-L: 1	ETSI EN 319 122-1 [1], clause A 1.1.2	as in Table A.1
Service: revocation values in long-term validation	shall be provided	1		as in Table 1
SPO: `SignedData.crls.crl`	conditioned presence	0 or 1	ETSI EN 319 122-1 [1], clause 4.4	as in Table 1
SPO: `SignedData.crls.other`	conditioned presence	0 or 1	ETSI EN 319 122-1 [1], clause 4.4	as in Table 1
SPO `revocation-values`	may be present	Build on E-C, E-X: 0 or 1 Build on E-X-Long, E-X-L: 1	ETSI EN 319 122-1 [1], clause A.1.2.2	as in Table A.1

Signature fields/Attributes/Services	Presence in E-A level	Cardinality	References	Additional requirements and notes
Service: add archive time-stamp	shall be provided	≥ 1	ETSI EN 319 122-1 [1], clause 5.6.1	
SPO: `archive-time-stamp-v3`	conditioned presence	≥ 0	ETSI EN 319 122-1 [1], clause 5.6.2	as in Table 1
SPO: `long-term-validation`	conditioned presence	≥ 0	ETSI EN 319 122-1 [1], clause A.2.5	as in Table 1

Annex B (informative): Change History

date	Version	Information about changes
November 2013	V0.0.3	Update of references and added clarification concerning LTA signatures containing already a `long-term-validation` attribute, adding a section on the signer attributes.
September 2014	V0.0.4	Update title and add document to include seals.
December 2014	V0.0.5	Changed content to CAdES forms and extensions, as agreed by ESI. Now this part does not contain the Baseline Profile anymore.
January 2015	V0.0.6	Implemented new introduction and scope in line with the strategy agreed by ESI on the scope of the standards. Implemented resolutions to comments to v0.0.5 regarding, among others to terminology (levels instead forms) and legacy signatures. Reviewed requirements for all the levels. Signer-attributes is not allowed anymore in BES, since it is deprecated.
February 2015	V0.0.7	The specification CAdES levels is made in single tables using the new notation.
February 2015	V0.0.8	Final editorial changes.
Mai 2015	V0.0.9	Resolution of comments after public review.
June 2015	V0.0.10	Small corrections in the table, addition of services for certificates and validation data for longterm validation in the tables, adding a new table for CAdES-E-A in annex A.

History

Document history		
V1.0.0	June 2015	EN Approval Procedure AP 20151028: 2015-06-30 to 2015-10-28