ETSI TS 119 122-3 V1.1.1 (2017-01)

Electronic Signatures and Infrastructures (ESI);
CAdES digital signatures;
Part 3: Incorporation of Evidence Record Syntax (ERS) mechanisms in CAdES

Reference
DTS/ESI-000120

Keywords
ASN.1, CAdES, electronic signature, profile, 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

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 (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.

Foreword

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

The present document is part 3 of a multi-part deliverable covering CAdES digital signatures. Full details of the entire series can be found in part 1 [4].

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

Evidence record syntax (ERS) allows to cover different data objects with a single time-stamp, and subsequently augment the lifetime of the evidence record (ER) by adding validation data to the previous time-stamp and adding new time-stamps. The aim of the present document is to provide clear indications how to bind an ERS to a CAdES signature which is covered by the ERS.

NOTE: ETSI EN 319 162-1 [i.5] and ETSI EN 319 162-2 [i.6] specify the use of ERS in ASiC.

1 Scope

The present document provides mechanism to incorporate evidence records in ASN.1 format within a CAdES signature as outlined in ETSI EN 319 122-1 [4], annex B. It specifies the attributes to be used and profiles the ERS standard (IETF RFC 4998 [2]) to provide clear rules how to incorporate ERS within a CAdES signature or a legacy CAdES signature.

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 https://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] IETF RFC 3161 (2001): "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)".

[2] IETF RFC 4998 (2007): "Evidence Record Syntax (ERS)".

[3] IETF RFC 5816 (2010): "ESSCertIDv2 Update for RFC 3161".

[4] 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 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 TR 119 001: "Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures; Definitions and abbreviations".

[i.2] ETSI TS 101 733: "Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)".

[i.3] ETSI EN 319 122-2: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 2: Extended CAdES signatures".

[i.4] ETSI TS 119 312: "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites".

[i.5] ETSI EN 319 162-1: "Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 1: Building blocks and ASiC baseline containers".

[i.6] ETSI EN 319 162-2: "Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 2: Additional ASiC containers".

[i.7] 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".

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.1], ETSI EN 319 122-1 [4] and the following apply:

archive-timestamp: timestamp which is used for long-term preservation purposes

EXAMPLE: An archive-timestamp can for example be a `TimeStampToken` according to IETF RFC 3161 [1] and updated by IETF RFC 5816 [3] or an `ArchiveTimeStamp` according to IETF RFC 4998 [2].

evidence-record: Evidence Record according to IETF RFC 4998 [2].

evidence-records attribute: unsigned attribute which contains one or more evidence-records as defined in the present document

evidence record renewal: either time-stamp renewal or hash-tree renewal within an evidence record

initial `ArchiveTimeStamp`: the first `ArchiveTimeStamp` instance of the first `ArchiveTimeStampChain` instance within the `ArchiveTimeStampSequence` instance

NOTE: `ArchiveTimeStamp`, `ArchiveTimeStampChain` and `ArchiveTimeStampSequence` are as defined in IETF RFC 4998 [2].

validation data: data that is used to validate a digital signature

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI TR 119 001 [i.1] and the following apply:

ER	Evidence Record
ERS	Evidence Record Syntax
TSU	Time Stamping Unit

4 General requirements

4.1 Introduction

This clause specifies mechanisms how to include validation data into the signature.

4.2 Inclusion of validation data within a `TimeStampToken` instance

When including validation data within a `TimeStampToken` instance according to IETF RFC 3161 [1] and updated by IETF RFC 5816 [3] one of the following methods shall be used:

1) adding the information in the `SignedData` of the timestamp token; or

2) adding the `certificate-values` attribute according to ETSI EN 319 122-1 [4], clause A.1.1.2 and the `revocation-values` attribute according to ETSI EN 319 122-1 [4], clause A.1.2.2 as unsigned attributes within the `TimeStampToken` instance.

Method 1) should be used.

4.3 Inclusion of validation data within CAdES signatures

The present document specifies two strategies for the inclusion of validation data within a CAdES signature, depending on whether attributes for long term availability, as defined in different versions of ETSI TS 101 733 [i.2], have already been added to the `SignedData`:

- If none of ATSv2 attributes (see clause A.2.4 of ETSI EN 319 122-1 [4]), or an earlier form of archive time-stamp as defined in ETSI TS 101 733 [i.2] or `long-term-validation` (see clause A.2.5 of ETSI EN 319 122-1 [4]) attributes is already present in any `SignerInfo` of the root `SignedData`, then the new validation material shall be included within the root `SignedData.certificates`, or `SignedData.crls` as applicable.

- If an ATSv2, or other earlier form of archive time-stamp or a `long-term-validation` attribute, is present in any `SignerInfo` of the root `SignedData` then the root `SignedData.certificates` and `SignedData.crls` contents shall not be modified. The new validation material shall be provided within the `TimeStampToken` instance of the latest archive time-stamp (which can be an ATSv2 or an ATSv3 as defined in clause 5.5.3 of ETSI EN 319 122-1 [4]) or within the latest `long-term-validation` attribute already contained in the `SignerInfo` as described in ETSI EN 319 122-1 [4], clause A.2.5.

OCSP responses shall be included as defined in clause 5.4.2 of ETSI EN 319 122-1 [4].

If the OCSP response is included within `SignedData.crls`, it shall be included as defined in clause 5.4.2.2 of ETSI EN 319 122-1 [4].

When generating a new attribute to include validation data, either initially when creating the signature or later when augmenting the signature, it shall be encoded in DER (see clause 4.7.1 of ETSI EN 319 122-1 [4]), whilst preserving the encoding of any signed field included in the attribute. The augmentation shall preserve the binary encoding of already present unsigned attributes and any component contributing to the archive time-stamp's message imprint computation input.

5 Attribute semantics and syntax

5.1 The evidence-records attributes

In the present document two attributes are described that allow to include an evidence record (ER) over the whole `SignedData` instance:

- The `internal-evidence-records` attribute (clause 5.2) protects the whole `SignedData` instance and is used in cases of attached signatures.

- The `external-evidence-records` attribute (clause 5.3) also protects the whole `SignedData` instance not containing an `eContent` element within `encapContentInfo` (a detached signature), and the external signed data.

The term "evidence-records attribute" is used to denote either one of these attributes.

Semantics

The evidence-records attribute shall be an unsigned attribute.

At most one of the `SignerInfo` instances within the `SignedData` instance shall contain evidence-records attributes. If the `SignerInfo` instance contains more than one evidence-records attribute, only the ER(s) in the latest added evidence-records attribute shall be updated.

NOTE 1: Updating one of the ER in the other evidence-records attributes will invalidate the ER(s) in the later added evidence-records attribute(s).

Once an evidence-records attribute is included within a `SignedData` instance, the only changes that might be applied to the `SignedData` instance are the renewal of the ER within the evidence-records attribute, the adding of a new ER within a new `AttributeValue` of the latest evidence record attribute or the adding of another evidence-records attribute. No other changes shall be applied to the `SignedData` instance.

Syntax

The `ContentInfo` instance shall be DER encoded before computing the hash.

The evidence-records attribute may contain one or more instances of `AttributeValue` type.

The evidence-records attribute should contain one instance of `AttributeValue` type.

If the evidence-records attribute contains more than one instance of `AttributeValue` type, the input of the message imprint computation of all initial `ArchiveTimeStamp` within each of the `AttributeValue` instances shall include at least exactly the same fields within the signature and the signed document. The parts of the reduced hash-tree not corresponding to the signature or the signed document may be different.

NOTE 2: Having more than one instance of `AttributeValue` type allows to have parallel evidence-records (from different TSAs or with different hash algorithms) protecting the same signature.

NOTE 3: This means that if a signature contains already an evidence-records attribute with more than one instance of `AttributeValue` type, and a new evidence-records attribute is added (with one or more instances of `AttributeValue` type) this new attribute covers amongst other information the whole previous evidence-records attribute, including all instances of `AttributeValue` type.

The evidence-records attribute value shall be an instance of `EvidenceRecord` ASN.1 type as defined in IETF RFC 4998 [2].

The `timeStamp` field of any `ArchiveTimeStamp` instance within the `EvidenceRecord` instance shall be of type `TimeStampToken` as defined in IETF RFC 3161 [1] and updated by IETF RFC 5816 [3].

Before adding a new `ArchiveTimeStamp` instance to the ER, i.e. during a Timestamp Renewal or a Hash-Tree Renewal, the validation data missing to validate the time-stamp within the latest `ArchiveTimeStamp` instance shall be included within the `TimeStampToken` of the latest `ArchiveTimeStamp` instance as described in clause 4.

Before covering a `SignedData` instance with an ER included in an evidence-records attribute, the `SignedData` shall be extended to include any validation data, not already present, which is required for validating all the included `SignerInfo` instances. Validation data may include certificates, CRLs, OCSP responses, as required to validate any signed object within the signature including the existing signature, counter-signatures, time-stamps, OCSP responses, certificates, attribute certificates and signed assertions. In the case that the validation data contains a Delta CRL, then the whole set of CRLs shall be included to provide a complete revocation list.

NOTE 4: Validation data already present for example in the time-stamp token need not be included again.

Before adding a new evidence-records attribute, all the missing validation data to validate all the evidence-records in the previous evidence-records attributes shall be added within the corresponding `timeStamp` field instance of the latest `ArchiveTimeStamp` instance in each evidence-record as described in clause 4.

5.2 The `internal-evidence-records` attribute

Semantics

The `internal-evidence-records` attribute incorporates an ER covering the `ContentInfo` instance of type `signed-data`, as specified in ETSI EN 319 122-1 [4], containing an `eContent` element within `encapContentInfo`.

Syntax

The `internal-evidence-records` attribute shall be identified by the `id-aa-er-internal` OID as defined in ERS (IETF RFC 4998 [2], appendix A).

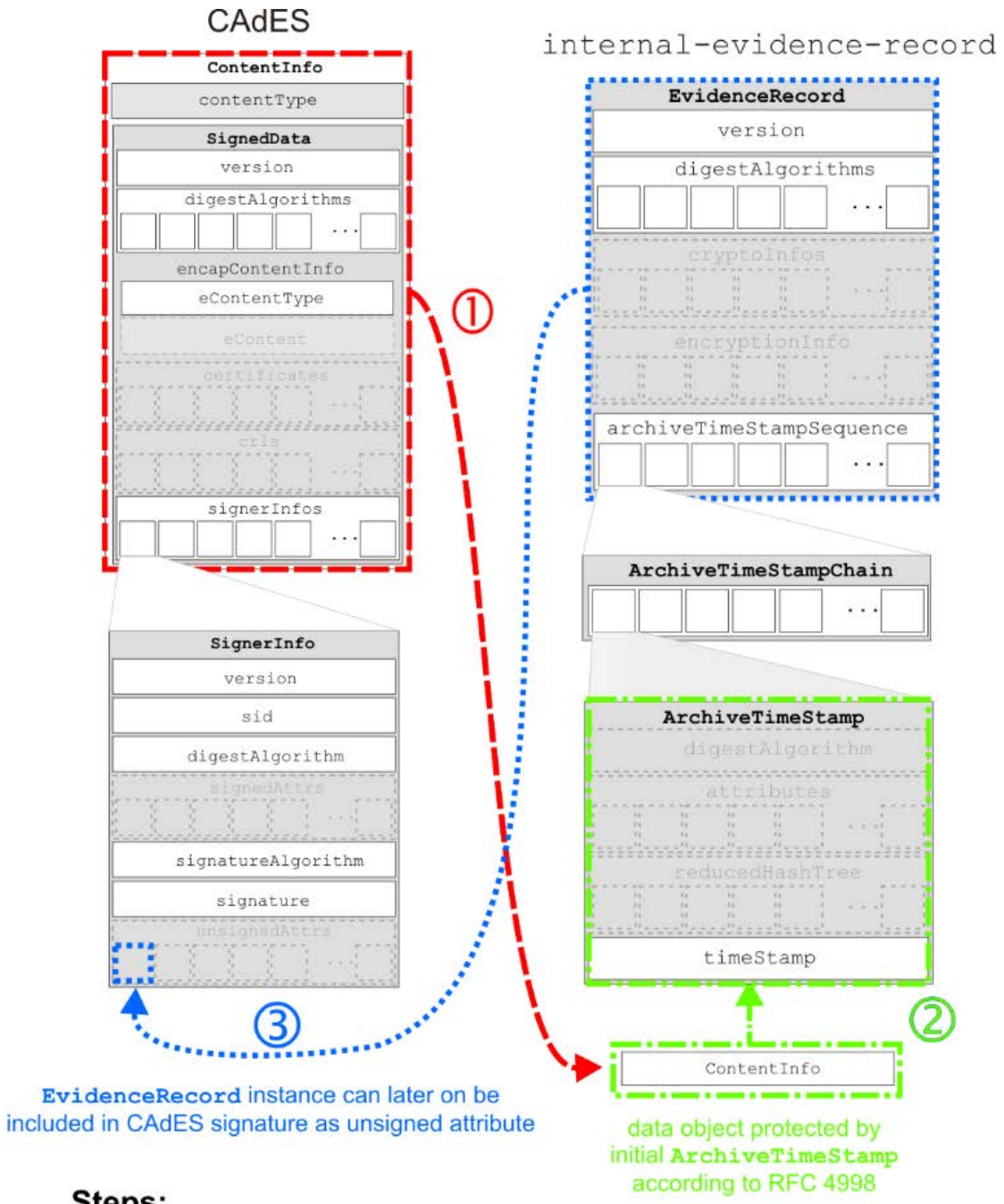
For the initial `ArchiveTimeStampSequence`,

1) if the initial `ArchiveTimeStamp` contains the `reducedHashtree` field, then the first component of the instance of `PartialHashtree` type shall contain in its object group at least the hash value of the `ContentInfo` instance of type `signed-data`;

2) if the initial `ArchiveTimeStamp` does not contain the `reducedHashtree` field, then the message imprint of the corresponding `TimeStampToken` shall be the hash value of the `ContentInfo` instance of type `signed-data`.

Illustration

Figure 1 illustrates the `internal-evidence-records` attribute.



Steps:

① the complete `ContentInfo` instance serves as input for the `messageImprint` computation of the initial `ArchiveTimeStamp` instance

② the `EvidenceRecord` instance is built based on this initial `ArchiveTimeStamp` instance

③ the `EvidenceRecord` instance can later on be included in CAdES signature as unsigned `internal-evidence-record` attribute

Figure 1: Illustration of `internal-evidence-records` attribute

5.3 The external-evidence-records attribute

Semantics

The external-evidence-records attribute incorporates an ER covering the ContentInfo instance of type signed-data, as specified in ETSI EN 319 122-1 [4], not containing an eContent element within encapContentInfo, i.e. in case of an external signature, and the external signed data.

Syntax

The external-evidence-records attribute shall be identified by the id-aa-er-external OID as defined in ERS (IETF RFC 4998 [2], appendix A).

For the initial ArchiveTimeStampSequence the initial ArchiveTimeStamp shall contain the reducedHashtree field. The first component of the instance of PartialHashtree type shall contain in its object group at least the hash value of the ContentInfo instance of type signed-data and the hash value of the externally signed content.

Illustration

Figure 2 illustrates the external-evidence-records attribute.

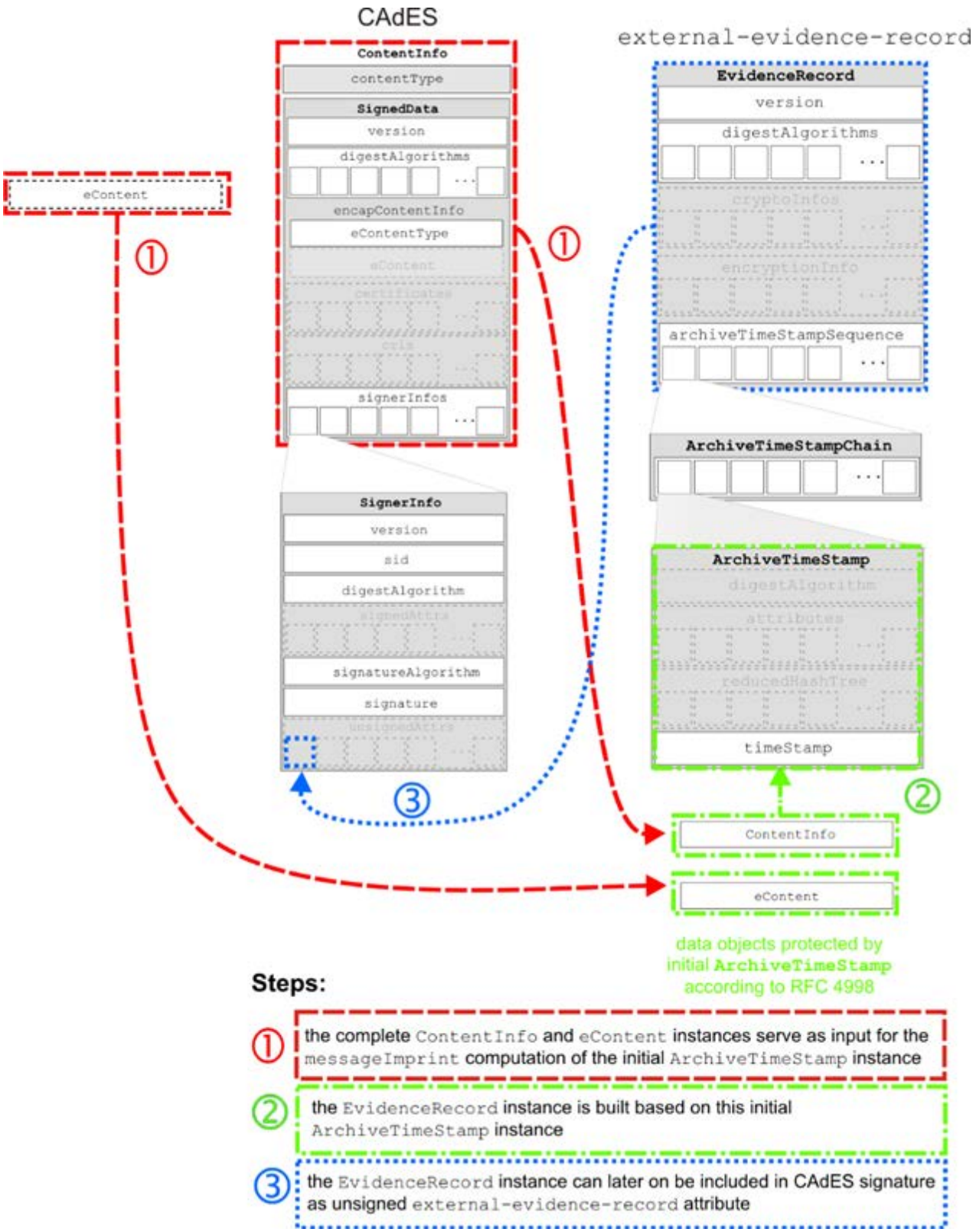


Figure 2: Illustration of `external-evidence-records` attribute

6 CAdES signature level including ERS

6.1 Overview

The present document specifies a new level for CAdES signatures including ERS.

Each level is created by a combination of attributes defined in ETSI EN 319 122-1 [4] and the present document.

6.2 General requirements

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

The signature shall contain a CMS `SignedData`, as defined in ETSI EN 319 122-1 [4], clause 4.4 and at least one `SignerInfo` (ETSI EN 319 122-1 [4], clause 4.6).

The algorithms and key lengths used to generate and augment digital signatures should be as specified in ETSI TS 119 312 [i.4].

NOTE: Cryptographic suites recommendations defined in ETSI TS 119 312 [i.4] can be superseded by national recommendations.

6.3 CAdES-E-ERS

CAdES-E-ERS may be built on all the levels described in ETSI EN 319 122-1 [4] or ETSI EN 319 122-2 [i.3].

Table 1: Requirements for CAdES-E-ERS

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

Signature fields/Attributes/Services	Presence in E-ERS level	Cardinality	References	Additional requirements and notes
content-reference	may be present	0 or 1	ETSI EN 319 122-1 [4], clause 5.2.11	
content-identifier	may be present	0 or 1	ETSI EN 319 122-1 [4], clause 5.2.12	
signature-time-stamp	shall be present	≥ 1	ETSI EN 319 122-1 [4], clause 5.3	f, 1, 4
complete-certificate-references	*	0 or 1	ETSI EN 319 122-1 [4], clause A.1.1.1	e
complete-revocation-references	*	0 or 1	ETSI EN 319 122-1 [4], clause A.1.2.1	
attribute-certificate-references	*	0 or 1	ETSI EN 319 122-1 [4], clause A.1.3	d, e
attribute-revocation-references	*	0 or 1	ETSI EN 319 122-1 [4], clause A.1.4	d
CAdES-C-timestamp	*	≥ 0	ETSI EN 319 122-1 [4], clause A.1.5.2	1
time-stamped-certs-crls-references	*	≥ 0	ETSI EN 319 122-1 [4], clause A.1.5.1	1
Service: certificate values in long-term validation	shall be provided	≥ 1		g, h
SPO: SignedData.certificates	conditioned presence	0 or 1	ETSI EN 319 122-1 [4], clause 4.4	i
SPO: certificate-values	*	0 or 1	ETSI EN 319 122-1 [4], clause A.1.1.2	
Service: revocation values in long-term validation	shall be provided	1		j,k
SPO: SignedData.crls.crl	conditioned presence	0 or 1	ETSI EN 319 122-1 [4], clause 4.4	l
SPO: SignedData.crls.other	conditioned presence	0 or 1	ETSI EN 319 122-1 [4], clause 4.4	m
SPO revocation-values	*	0 or 1	ETSI EN 319 122-1 [4], clause A.1.2.2	
archive-time-stamp-v3	*	≥ 0	ETSI EN 319 122-1 [4], clause 5.5.3	n
Service: ERS inclusion	shall be provided	≥ 1	Clause 5.1	o, p
SPO: internal-evidence-records	conditioned presence	≥ 0	Clause 5.2	q
SPO external-evidence-records	conditioned presence	≥ 0	Clause 5.3	r

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 at least a certified signer attribute (certifiedAttributesV2 as defined in clause 5.2.6.1 of ETSI EN 319 122-1 [4]) or a signed assertion (signedAssertions as defined in clause 5.2.6.1 of ETSI EN 319 122-1 [4]) 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 [4].

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 `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.

o) Requirement for Service: ERS inclusion. Before generating and incorporating an evidence-records 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.

p) Requirement for Service: ERS inclusion. Only one evidence-records attribute should be included.

q) Requirement for SPO: `internal-evidence-records`. In case a signature is attached, the `internal-evidence-records` attribute shall be used.

r) Requirement for SPO: `external-evidence-records`. In case a signature is detached, the `external-evidence-records` attribute shall be used.

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.7].

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

History

Document history		
V1.1.1	January 2017	Publication