ETSI TS 103 173 V2.1.1 (2012-03)

Technical Specification

Electronic Signatures and Infrastructures (ESI); CAdES Baseline Profile

Reference

RTS/ESI-000105

Keywords

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

Important notice

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

Introduction

TS 101 733 [1] (CAdES henceforth) specifies formats for Advanced Electronic Signatures built on CMS [2]. That document defines a number of signed and unsigned optional signature properties, resulting in support for a number of variations in the signature contents and powerful processing requirements.

In order to maximise interoperability in communities applying CAdES to particular environments it is necessary to identify a common set of options that are appropriate to that environment. Such a selection is commonly called a profile.

The present document profiles TS 101 733 [1] signatures contexts where AdES signatures are used and in particular its use in the context of the "Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market" [i.7] (EU Services Directive henceforth).

1 Scope

The present document defines a baseline profile for CAdES that provides the basic features necessary for a wide range of business and governmental use cases for electronic procedures and communications to be applicable to a wide range of communities when there is a clear need for interoperability of AdES signatures used in electronic documents to be interchanged across borders. In particular it takes into account eSignature needs in the context of the EU Services Directive [i.7].

The present document defines four different conformance levels addressing incremental requirements to maintain the validity of the signatures over the long term, in a way that all the requirements addressed at a certain level are always addressed also by the levels above. Each level requires the presence of certain CAdES attributes, suitably profiled for reducing the optionality as much as possible and referring to the forms that are specified in CAdES [1].

Clause 4 identifies the four conformance levels and shows how these levels might encompass the life cycle of the electronic signatures.

Clause 5 provides details on the way that the requirements will be specified throughout the present document.

Clause 6 profiles short-term related CAdES attributes.

Clause 7 profiles a CAdES signature for which a Trust Service Provider has generated a trusted token (time-mark or time-stamp token) proving that the signature itself actually existed at a certain date and time.

Clause 8 profiles long-term related CAdES attributes tackling the long term availability of the signature validation material.

Clause 9 profiles long-term related CAdES attributes tackling the long term availability and integrity of the signature validation material.

NOTE: The present document makes use of certain verbal forms (e.g. **may**, **shall**, **shall not** and **should**) as key words to signify requirements, conforming to ETSI Drafting Rules, clause 14a [i.6].

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

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

2.1 Normative references

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

[1] ETSI TS 101 733 (V2.1.1): "Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)".

NOTE: Available at "http://www.etsi.org/deliver/etsi_ts/101700_101799/101733/.

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

NOTE: Obsoletes RFC 3852.

[3] IETF RFC 2634: "Enhanced Security Services for S/MIME".

NOTE: Available at http://tools.ietf.org/rfcmarkup/2634.

[4] IETF RFC 5035: "Enhanced Security Services (ESS) Update: Adding CertID Algorithm Agility".

NOTE: Available at http://tools.ietf.org/rfcmarkup/5035.

[5] ETSI TS 102 176-1: "Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms".

NOTE: Available at http://www.etsi.org/deliver/etsi_ts/102100_102199/10217601/.

[6] ECRYPT II (European Network of Excellence in Cryptology II): "ECRYPT II Yearly Report on Algorithms and Keysizes".

2.2 Informative references

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] Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market.

[i.2] Commission Decision 2009/767/EC of 16 October 2009 amended by CD 2010/425/EU of 28 July 2010 setting out measures facilitating the use of procedures by electronic means through the 'points of single contact' under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market.

[i.3] ETSI TS 102 231: "Electronic Signatures and Infrastructures (ESI); Provision of harmonized Trust-service status information".

[i.4] ETSI TS 101 533-1: "Electronic Signatures and Infrastructures (ESI); Data Preservation Systems Security; Part 1: Requirements for Implementation and Management".

[i.5] ETSI TS 102 640-1: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 1: Architecture".

[i.6] ETSI Drafting Rules (EDRs).

NOTE: Contained in the ETSI Directives: http://portal.etsi.org/Directives/home.asp.

[i.7] Commission Decision 2011/130/EU of 25 February 2011; establishing minimum requirements for the cross-border processing of documents signed electronically by competent authorities under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market (notified under document C(2011) 1081).

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

generator: any party which creates, or adds attributes to, a signature

NOTE: This may be the signatory or any party which initially verifies or further maintains the signature.

protocol element: element of the protocol which may be including data elements and/or elements of procedure

service element: element of service that may be provided using one or more protocol elements

NOTE: All alternative protocol elements provide an equivalent service to the users of the protocol.

trust service provider: body operating one or more (electronic) Trust Services

NOTE: See [i.3].

verifier: entity that validates or verifies an electronic signature

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in CAdES [1] and the following apply:

TSL	Trust Status List

4 Conformance Levels

The present document defines four conformance levels as indicated below.

Applications managing signatures conformant to requirements specified in clause 6 may claim **B-Level** (basic Level) conformance.

Applications managing signatures conformant to B-Level and also conformant to requirements specified in clause 7 may claim **T-Level** (Trusted time for signature existence) conformance.

Applications managing signatures conformant to T-Level and also conformant to requirements specified in clause 8 of the present document may claim **LT-Level** (Long Term level) conformance.

Applications managing signatures conformant to LT-Level and also conformant to requirements specified in clause 9 of the present document may claim **LTA-Level** (Long Term with Archive time-stamps) conformance.

These conformance levels are defined for encompassing the life cycle of electronic signature, namely:

a) B-Level profiles incorporation of signed and some unsigned properties when the signature is actually generated.

NOTE 1: It is considered that this level is sufficient to conform to the Commission Decision 2011/130/EU of 25 February 2011 [i.7].

b) T-Level profiles the generation and inclusion, for an existing signature, of a trusted token proving that the signature itself actually existed at a certain date and time.

c) LT-Level profiles the incorporation of all the material required for validating the signature in the signature. This level is understood to tackle the long term availability of the validation material.

d) LTA-Level profiles the incorporation of time-stamp tokens that allow validation of the signature long time after its generation. This level is understood to tackle the long term availability and integrity of the validation material.

NOTE 2: The levels b) to d) are appropriate where the technical validity of signature needs to be preserved for a period of time after signature creation where certificate exipiration, revocation and/or algorithm obsolescence is of concern. The specific level applicable depends on the context and use case.

All conformance levels up to LTA uses attributes defined in CAdES [1].

When signed data is exchanged between parties the sender **should** use at least signatures conforming to a level that allows the relying parties to trust the signature at the time the exchange takes place.

NOTE 3: Archiving or preservation of electronic signatures over long term requires in general conformance to LTA level. The use of LTA-level is considered an appropriate preservation and transmission technique for signed data. Conformance to lower level is sufficient when combined with appropriate additional protection techniques such as use of systems compliant to TS 101 533-1 [i.4] .

NOTE 4: The assessment of the effectiveness of other preservation and transmission techniques for signed data are out of the scope of the present document. The reader is advised to consider legal instruments in force and related standards such as TS 101 533-1 [i.4] or TS 102 640-1 [i.5] to evaluate their appropriateness.

5 General requirements

5.1 Algorithm requirements

Generators are referred to applicable national laws regarding algorithms and key lengths.

Generators are also recommended to take into account the latest version of TS 102 176-1 [5] for guideline purposes and the latest ECRYPT2 D.SPA.13 [6] yearly report for further recommendations, when selecting algorithms and key lengths.

MD5 algorithm **shall not** be used as digest algorithm.

5.2 Compliance requirements

Profiles in the present document define requirements for generator of CAdES signatures [1].

The present document defines a profile that specifies which elements/properties **shall** and which **may** be present in a CAdES signature.

A verifier **shall** be able to accept a signature containing any elements/properties conformant to CAdES [1], but the present document does not specify any processing requirement on such elements/properties present in the signature as it is meant to be used together with a specification describing processing during signature validation.

Requirements are grouped in two different categories, each one having its corresponding identifier. Table 1 defines these categories and their identifiers.

Table 1: Requirement categories

Identifier	Requirement on generator
M	Generator **shall** include the element in the signature.
O	Generator **may** include the element in the signature.

Optional elements defined in CAdES [1] but not specified in the present document are treated as "O" as above.

Certain service elements **may** be provided by different protocol elements at user's choice. In these cases the semantics of M and O defined in table 1 depend on the requirement for the service element itself. Tables 2 and 3 (each one applies to a different requirement on the service element) define these semantics.

Table 2: Requirements for mandatory service with choices

Requirement Identifier for the Service/Protocol element	Requirement on generator
Service = M	Generator **shall** provide the service by including one protocol element chosen from the list of choices.
Protocol Choice = O	Generator **may** use this protocol element for providing the mandatory service elements.

Table 3: Requirements for optional service with choices

Requirement Identifier for the Service/Protocol element	Requirement on generator
Service = O	Generator **may** provide the service by including one protocol element chosen from the list of choices.
Protocol Choice = O	If the generator decides to provide the service, then it **may** use this protocol element.

The present document shows new requirements for each service and protocol element in tabular form. Below follows the structure of the table.

Table 4: Requirements for optional service with choices

Service/Protocol element	Reference	Requirement on generator	Notes/Additional requirements
Service:			
Choice 1			
Choice 2			

Column **Service/Protocol element** will identify the service element or protocol element the requirement applies to. Service elements that **may** be implemented by different protocol elements (i.e. users **may** make a choice on several protocol elements) build tables with more than one row.

Column **Reference** will reference the relevant clause of the standard where the element is first defined. The reference is to CAdES [1], except where explicitly indicated otherwise.

Column **Requirement on generator** will contain an identifier of the requirement, as defined in table 1, bound to the corresponding protocol element for the generator.

Column **Notes/Additional requirements** will contain numbers referencing notes and/or letters referencing additional requirements. Both notes and additional requirements are listed below the table.

Profiles **may** be affected by applicable regulations; hence implementers **should** check any national regulation that may affect these profiles.

6 Requirements for B-Level Conformance

This clause defines requirements that CAdES signatures claiming conformance to the B-Level have to fulfil.

This clause actually profiles CAdES-BES (when `the signature-policy-id attribute is not present`) and CAdES-EPES (when `the signature-policy-id attribute` is present) signatures.

In consequence, the following CAdES attributes are addressed directly in this clause: `content-type, signing-time and signing-certificate.` Further `message-digest, signature-policy-identifier, counter-signature, content-reference, content-identifier, content-hints, commitment-type-indication, signer-location, signer-attributes, content-time-stamp, mime-type` are inherently addressed.

Clause 6.1 profiles attributes defined in CMS [2], namely: content-type and signing-certificate.

Clause 6.2 profiles attributes defined in ESS [4], namely: signing-certificate.

No further requirements are defined by the present document for the rest of the attributes specified by CAdES [1]. In the case an optional unsigned attribute is incorporated in the signature, DER encoding **shall** be used for this attribute.

6.1 Attributes defined in CMS Signature

6.1.1 Content type

Table 5

Service/Protocol element	CMS [2] Reference	Generator Requirement	Additional requirements/notes
`ContentType`	Clause 11.1	M	a

Additional requirement:

a) The generator **shall** include the ContentType attribute with value id-data.

6.1.2 Signing time

Table 6

Service/Protocol element	CMS [2] Reference	Generator requirement	Additional requirements/notes
`SigningTime`	Clause 11.3	M	a

Additional requirement:

a) The generator shall include the claimed UTC time expressed as in [2] clause 11.3 when the signature was generated as content of this element.

6.1.3 Placement of the signing certificate

Table 7

Service/Protocol element	CMS [2] Reference	Generator requirement	Additional requirements/notes
`SignedData.certificates`	Clause 5.1	M	a, b, c

Additional requirements:

a) The generator **shall** include the signer certificate in the SignedData.certificate field.

b) In order to facilitate path building, the generator **should** include in the SignedData.certificate field all certificates not available to verifiers that can be used during path building. In the case of signature based on qualified certificates and whose verification is expected to be based on TSLs (in particular on Trusted Lists as defined in CD 2009/767/EC amended by CD 2010/425/EU [i.2])", the generator **should** include all intermediary certificates forming a chain between the signer certificate and a CA present in the TSL which are not available to verifiers.

NOTE 1: A certificate is considered available to the verifier if reliable information about its location is known and allows automated retrieval of the certificate (for instance through an Authority Info Access Extension or equivalent information present in a TSL).

NOTE 2: In the general case, different verifiers can have different trust parameters and can validate the signer certificate through different chains. Therefore, the generator may not know which certificates will be relevant for path building. However, in practice, such certificates can often clearly be identified. In this case, it is advised that the generator include them unless they can be automatically retrieved by verifiers. In the specific case of a signature meant to be validated through TSL, it is advised to include at least the unavailable intermediary certificates up to but not including the Cas present in the TSLs, since the TSL is information that is shared globally by all verifiers.

c) The requirements a) and b) cannot be satisfied in the case the SignedData.certificate field is used in the computation of a digest included in existing signatures such that the addition of a certificate in this field would invalidate previous signatures (for instance, the case of co-signing a CAdES-A signature).

6.2 Attributes defined in ESS

6.2.1 Signing certificate

Table 8

Service/Protocol element	ESS [3, 4] reference	Generator Requirement	Additional requirements/notes
Service: protection of signing certificate		M	
`ESS signing-certificate`	ESS [3], Clause 5.4	O	a, b
`ESS signing-certificate` v2	ESS [4], Clause 4	O	a, b

Additional requirement:

a) The generator **shall** use either the signing certificate or the signing-certificate v2 attribute, depending on the hash function using, in accordance with ESS [4], clause 2.

b) The generator **should** migrate to the use of ESS signing-certificate v2 in preference to ESS signing-certificate in line with the guidance regarding limited lifetime for the use of SHA-1 given in clause 9.2 of TS 102 176-1 [5].

7 Requirements for T-Level Conformance

This clause defines those requirements that CAdES signatures conformant to B-Level, have to fulfil for also being conformant to T-Level. In consequence, CAdES signatures claiming conformance to the T-Level of the present document **shall** be built on signatures conformant to the B-Level.

A CAdES signature conformant to T-Level **shall** be a signature conformant to B-Level for which a Trust Service Provider [i.3] has generated a trusted token (time-mark or time-stamp token) proving that the signature itself actually existed at a certain date and time.

NOTE: CAdES signatures conformant to T-Level of the present document are, in consequence, CAdES-T signatures suitably profiled as per the requirements defined in this clause.

Table 9 further profiles the provision of the trusted token that proves existence of the signature at a certain date and time.

Table 9

Service/Protocol element	CAdES [1] Reference	Generator Requirement	Additional requirements/notes
Service: trusted time for existence of the signature		M	
`Signature-time-stamp attribute`	Clause 6.1	O	a, b, c
`Time mark`	Clause 4.4.1	O	d

Additional requirements

a) The present document recommends usage of time-stamps as attestation of the time for existence of the signature instead of time-marks.

b) A CAdES-T claiming conformance to the present document **may** contain several `signature-time-stamp attributes.`

c) The generator **shall** use DER encoding for any signature-time-stamp attribute.

d) If a time-mark is used, then no additional attribute is incorporated into the signature. It is the responsibility of the TSP generating the time-mark to provide the needed trust on the signature time.

8 Requirements for LT-Level Conformance

This clause defines those requirements that CAdES signatures conformant to T-Level, have to fulfil to also be conformant to LT-Level. In consequence, CAdES signatures claiming conformance to the LT-Level of the present document **shall** be built on signatures conformant to the T-Level.

CAdES signatures conformant to LT-Level **shall not** incorporate any of the following unsigned attributes: complete-certificate-references, complete-revocation-references, attribute-certificate-references, attribute-revocation-references, `CadES-C-time-stamp, time-stamped-certs-crls-references`, certificate-values, revocation-value, and archive-time-stamp.

NOTE 1: By doing so, the present document eliminates a high degree of optionality.

NOTE 2: The present document uses CAdES version 2.1.1 [1] which defines the new attribute long-term-validation intended to replace old validation material attributes.

CAdES signatures conformant to LT-Level are built by direct incorporation to CAdES-T signatures conformant to the T-Level, a long-term-validation attribute containing values of certificates and values of certificate revocation status used to validate the signature.

NOTE 3: CAdES signatures conformant to LT-Level of the present specification are, in consequence, CAdES-LT signatures suitably profiled as per the requirements defined in this clause.

8.1 Certificate values

Table 10

Service/Protocol element	CAdES [1] Reference	Generator Requirement	Additional requirements/notes
Service: certificate values in long-term-validation	Clause 6.5	M	
`Long-term-validation.extraCertificates`	Clause 6.5.1	O	a, b, c, d

Additional requirements:

a) 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, and for validating any time-stamp token's signing certificate (i.e. a TSA certificate) already incorporated to the signature.

b) In situations different than those ones identified in clause 6.1.3 of the present document requirements a) and b): applications **should** include certificate values within long-term-validation.extraCertificates.

c) The present document recommends to avoid duplication of certificate values within the signature.

d) The generator **shall** use DER encoding for the attribute.

8.2 Revocation values

Table 11

Service/Protocol element	CAdES [1] Reference	Generator Requirement	Additional requirements/notes
Service:revocation values in long-term-validation	Clause 6.5	M	a, b, c, d
Long-term)validation.extraRevocation. CertificateList	Clause 6.5.1	O	
Long-term)validation.extraRevocation. OtherRevocationInfoFormat	Clause 6.5.1	O	

Additional requirements:

a) 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 present in the signature, and for validating any time-stamp token's signing certificate (i.e. a TSA certificate) already incorporated to the signature.

b) Applications **should** include certificate status values within `long-term-validation.extraRevocation` instead within `SignedData.crls.`

c) The present document recommends to avoid duplication of revocation values within the signature.

d) The generator **shall** use DER encoding for the revocation-values attribute.

9 Requirements for LTA-Level Conformance

This clause defines those requirements that CAdES signatures conformant to LT-Level, have to fulfil to also be conformant to LTA-Level. In consequence, CAdES signatures claiming conformance to the LTA-Level of the present document **shall** be built on signatures conformant to the LT-Level.

A CAdES signature conformant to LTA-Level **shall** be a signature conformant to LT-Level to which one or more `long-term-validation attribute` with a poeValue has been incorporated.

NOTE 1: CAdES signatures conformant to LTA-Level of the present document are, in consequence, CAdES-LT signatures suitably profiled as per the requirements defined in this clause.

NOTE 2: As stated in CAdES [1], CAdES-LT form with a poeValue may help to validate the signature beyond any event that may limit its validity.

Table 12

Service/Protocol element	CAdES [1] Reference	Generator requirement	Additional requirements/notes
Service: poe value in long-term-validation	Clause 6.5	M	
long-term-validation.poeValue.timeStamp	Clause 6.5.1	O	a, b, c, 1, 2
Long-term-validation.poeValue.evidenceRecord	Clause 6.5.1	O	

Additional requirements:

a) Signatures conformant to LTA-level **may** have more than one `long-term-validation attribute each one containing a poeValue.`

b) Before generating and incorporating an archive-time-stamp attribute, applications claiming conformance to the present document, **shall** include all the validation material, which are not already in the signature, required for verifying the signature. This validation material includes all the certificates and all certificate status information (like CRLs or OCSP responses) required for:

- validating the signing certificate;
- validating any attribute certificate present in the signature;
- and validating any time-stamp token's signing certificate (i.e. a TSA certificate) already incorporated in the signature (including, of course, `any previous long-term-validation`).

This validation material **should** be incorporated within long-term-validation.extraCertificates and long-term-validation.extraRevocation.

c) The generator **shall** use DER encoding for any long-term-validation attribute.

History

Document history		
V1.1.1	September 2011	Publication
V2.1.1	March 2012	Publication