INTERNATIONAL STANDARD

ISO 14533-1

First edition
2012-09-15

Processes, data elements and documents in commerce, industry and administration — Long term signature profiles —

Part 1: Long term signature profiles for CMS Advanced Electronic Signatures (CAdES)

Processus, éléments d'informations et documents dans le commerce, l'industrie et l'administration — Profils de signature à long terme —

Partie 1: Profils de signature à long terme pour les signatures électroniques avancées CMS (CAdES)

Reference number
ISO 14533-1:2012(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO 14533-1 was prepared by Technical Committee ISO/TC 154, *Processes, data elements and documents in commerce*.

ISO 14533 consists of the following parts, under the general title *Processes, data elements and documents in commerce, industry and administration — Long term signature profiles*:

— *Part 1: Long term signature profiles for CMS Advanced Electronic Signatures (CAdES)*

— *Part 2: Long term signature profiles for XML Advanced Electronic Signatures (XAdES)*

Introduction

The purpose of this part of ISO 14533 is to ensure the interoperability of implementations with respect to long term signatures that make electronic signatures verifiable for a long term. Long term signature specifications referenced by each implementation cover CMS Advanced Electronic Signatures (CAdES) developed by the European Telecommunications Standards Institute (ETSI).

Processes, data elements and documents in commerce, industry and administration — Long term signature profiles —

Part 1: Long term signature profiles for CMS Advanced Electronic Signatures (CAdES)

1 Scope

This part of ISO 14533 specifies the elements, among those defined in CMS Advanced Electronic Signatures (CAdES), that enable verification of a digital signature over a long period of time.

It does not give new technical specifications about the digital signature itself, nor new restrictions of usage of the technical specifications about the digital signatures which have already existed.

NOTE CMS Advanced Electronic Signatures (CAdES) is the extended specification of Cryptographic message syntax (CMS), used widely.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ETSI TS 101 733 v1.8.1 (2009-11), *Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)* [1]

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
long term signature
signature that is made verifiable for a long term by implementing measures to enable the detection of illegal alterations of signature information, including the identification of signing time, the subject of said signature, and validation data

3.2
profile
rule used to ensure interoperability, related to the optional elements of referenced specifications, the range of values, etc.

3.3
required level
level of requirement for implementing each element constituting a profile

[1] Available from http://pda.etsi.org/pda/queryform.asp

3.4
cryptographic message syntax
CMS
syntax pertaining to the signature, digest, authentication, and encryption of a given message

NOTE Cryptographic message syntax is defined in IETF RFC 5652.

3.5
CMS advanced electronic signature
CAdES
electronic signature defined in ETSI TS 101 733 for which the signer can be identified and any illegal data alteration detected

3.6
CAdES with time
CAdES-T
CMS advanced electronic signature defined in ETSI TS 101 733 with information to ascertain signing time

EXAMPLE Signature timestamp.

3.7
archival CAdES
CAdES-A
CMS advanced electronic signature defined in ETSI TS 101 733 with information that enables the detection of any illegal alterations of information pertaining to the signature, including the subject of the signature and validation data

EXAMPLE Archive timestamp.

3.8
content information
data structure that defines the content in CMS

3.9
signed data
data structure that defines the signed data in CMS or related data

3.10
signerinfo
data structure that defines the signature information for each signer or related data

3.11
signed attribute
signature information that is the subject of a signature

3.12
unsigned attribute
signature information that is not the subject of a signature

NOTE The signature timestamp and archive timestamp are unsigned attributes.

3.13
validation data
certificate and revocation information used to validate a signature and timestamp

3.14
timestamping authority
TSA
trusted third party commissioned to provide proof that certain data existed prior to a certain point in time

3.15
timestamp token
TST
data object that binds a representation of a datum to a particular time, thus establishing evidence that the datum existed before that time

3.16
signature timestamp
timestamp affixed to a signature value in order to identify the time when the signature existed

3.17
archive timestamp
timestamp affixed to information pertaining to a signature, including the subject of the signature and validation data, in order to enable the detection of any illegal alteration

3.18
trust anchor
origin of trust provided in the form of a public key certificate or public key used by the validator to validate an electronic signature, and generally a public key certificate issued by a trusted root certification authority

3.19
trusted third party
TTP
security authority or its agent entrusted by another entity in connection with activities related to security

3.20
certification authority
CA
centre that is entrusted with the development and assignment of public key certificates

NOTE Certification authorities can, at their discretion, develop and assign keys to entities.

3.21
certificate
information on the publicly disclosed key as a part of an asymmetric key pair for an entity, signed by a certification authority to prevent forgery

3.22
attribute certificate
certificate containing the job, qualification, position, and other attributes and attribute values

3.23
revocation information
information issued by a certification authority with respect to a certificate revocated within the effective period

NOTE This information can be collated to determine whether the certificate is still in force.

3.24
enhanced security service
ESS
optional enhanced service related to a signature including, but not limited to, information identifying SigningCertificate and information showing the type of signature

4 Symbols

The following symbols are used for the “required level”.

— C Conditional

— M Mandatory

— O Optional

5 Requirements

5.1 The generation or validation of CAdES-T data conforms to this part of ISO 14533 provided that the following requirements are met:

a) all processing of elements whose required level is “Mandatory” in the CAdES-T profile, as specified in this part of ISO 14533, shall be included;

b) detailed specifications pertaining to the processing of any element whose required level is “Conditional” in the CAdES-T profile, as specified in this part of ISO 14533, shall be provided.

5.2 The generation or validation of CAdES-A data conforms to this part of ISO 14533 provided that the following requirements are met:

a) all processing of elements whose required level is “Mandatory” in the CAdES-A profile, as specified in this part of ISO 14533, shall be included;

b) detailed specifications pertaining to the processing of any element whose required level is “Conditional” in the CAdES-A profile, as specified in this part of ISO 14533, shall be provided.

5.3 When first-party conformity assessment is used, the implementer shall make a declaration of conformity to this part of ISO 14533 by disclosing the supplier’s declaration of compliance and its attachment (see Annex A) containing a description of implementation status (and the specifications for any elements “Conditional”).

NOTE Figure 1 shows the positioning of the generation and validation of CAdES-T data and CAdES-A data.

6 Long term signature profiles

6.1 Defined profiles

In order to make electronic signatures verifiable for a long term, signing time shall be identifiable, any illegal alterations of information pertaining to signatures, including the subject of information and validation data, shall be detectable, and interoperability ensured. To meet these requirements, this part of ISO 14533 defines the following two profiles with respect to CAdES:

a) CAdES-T profile: a profile pertaining to the generation and validation of CAdES-T data;

b) CAdES-A profile: a profile pertaining to the generation and validation of CAdES-A data.

Figure 1 shows the relation between CAdES-T data and CAdES-A data.

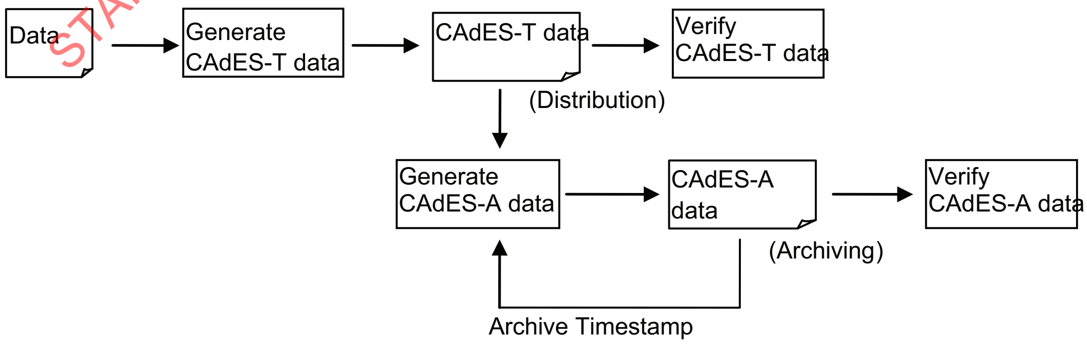

Figure 1 — Relation between CAdES-T data and CAdES-A data

6.2 Representation of the required level

This part of ISO 14533 defines the following representation methods for the required level (as a profile) of each element constituting CAdES-T data and CAdES-A data.

a) Mandatory (M) Elements whose required level is “Mandatory” shall be implemented without fail. If such an element has optional subelements, at least one subelement shall be selected. Any element whose required level is “Mandatory” and is one of the subelements of an optional element shall be selected whenever the optional element is selected.

b) Optional (O) Elements whose required level is “Optional” may be implemented at the discretion of the implementer.

c) Conditional (C) Elements whose required level is “Conditional” may be implemented at the discretion of the implementer, provided that detailed specifications for the processing thereof are provided separately.

6.3 Standard for setting the required level

The required level of each element constituting CAdES-T data and CAdES-A data shall be set in accordance with the following requirements.

a) The required level shall be “Mandatory” for elements whose required level is “Mandatory” in the definition of CAdES, and those necessary for the generation and validation of long term signatures. The elements whose required level is “Optional” in the definition of CAdES are defined as “Mandatory”, “Optional” or “Conditional”.

b) The required level shall be “Conditional” for externally defined elements.

EXAMPLE OtherCertificateFormat.

c) The required level shall be “Conditional” for elements intended to interact with a certain application.

EXAMPLE ContentReference.

d) The required level shall be “Conditional” for elements with an operation-dependent factor.

EXAMPLES Attribute certificate; time mark.

NOTE The archiving-type timestamp defined in ISO/IEC 18014-2 is included in “Time mark or other method.”

e) The required level shall be “optional” for elements only containing reference information.

6.4 Action to take when an optional element is not implemented

The following action shall be taken when the CAdES data used in a validation transaction contains an unimplemented element.

a) When the required level of an upper-level element is mandatory and one or more subordinate optional elements shall be selected, or one or more relevant optional elements shall be selected, the validator shall be cautioned that validation requires implementation of said element(s); otherwise, validation cannot be performed.

EXAMPLE In a validation transaction, a BasicOCSPResponse element is detected where only the processing of CertificateList elements, among all other optional elements in RevocationValues, is implemented.

b) When CounterSignature is an unimplemented element, the validator shall be cautioned that validation requires implementation of said element; otherwise, validation cannot be performed.

c) Optional elements other than those specified above may be ignored for implementation.

6.5 CAdES-T profile

6.5.1 General

The required levels of constituent elements of CAdES-T data are specified in 6.5.2 to 6.5.4.

6.5.2 Content information

Table 1 specifies the required level of each constituent element of Content information.

Table 1 — Content information

Element	Required level	Value	ETSI TS 101 733 v1.8.1 Reference
ContentType	M	Id-signedData	5.3
Content	M	SignedData	5.3

6.5.3 Signed data and Signer Info

Tables 2 and 3 specify the required level of each constituent element of Signed data and Signer Info.

Table 2 — Signed data

Element	Required level	ETSI TS 101 733 v1.8.1 Reference
CMSVersion	M	5.4
DigestAlgorithmIdentifiers	M	5.4
EncapsulatedContentInfo	M	5.4
eContentType	M	5.4
eContent	O	5.4
CertificateSet (Certificates)	O	5.4
Certificate	O	5.4
AttributeCertificateV2	C	5.4
OtherCertificateFormat	C	5.4
RevocationInfoChoices (crls)	O	5.4
CertificateList	O	5.4
OtherRevocationInfoFormat	C	5.4
SignerInfos	M	5.4
single	O	5.4
parallel	O	5.4

Table 3 — Signer Info

Element	Required level	ETSI TS 101 733 v1.8.1 Reference
CMSVersion	M	5.6
SignerIdentifier	M	5.6
IssuerAndSerialNumber	O	5.6
SubjectKeyIdentifier	O	5.6
DigestAlgorithmIdentifier	M	5.6
SignedAttributes	M	5.6
SignatureAlgorithmIdentifier	M	5.6
SignatureValue	M	5.6
UnsignedAttributes	M	5.6

6.5.4 Signed attribute and unsigned attribute

Tables 4 and 5 specify the required levels of elements that constitute signed attributes and unsigned attributes. The required level shall be “Conditional” for any signed and unsigned attribute elements not listed in Tables 4 and 5.

NOTE Unsigned attribute elements not listed in Tables 4 and 5 include, but are not limited to, CompleteCertificateReferences and CompleteRevocationReferences set forth in Table 6. CAdES-T data to which CompleteCertificateReferences and CompleteRevocationReferences are added can be made compliant with the CAdES-T profile by separately providing for the processing of these elements.

Table 4 — Signed Attributes

Element	Required level	ETSI TS 101 733 v1.8.1 Reference
ContentType	M	5.7.1
MessageDigest	M	5.7.2
SigningCertificateReference	M	5.7.3
ESS SigningCertificate	O	5.7.3.1
ESS SigningCertificate v2	O	5.7.3.2
OtherSigningCertificate	C	5.7.3.3
SignaturePolicyIdentifier	C	5.8.1
SigningTime	O	5.9.1
ContentReference	C	5.10.1
ContentIdentifier	C	5.10.2
ContentHints	C	5.10.3
CommitmentTypeIndication	C	5.11.1
SignerLocation	C	5.11.2.
SignerAttribute	C	5.11.3
ContentTimestamp	C	5.11.4

Table 5 — Unsigned Attributes

Element	Required level	ETSI TS 101 733 v1.8.1 Reference
CounterSignature	O	5.9.2
Trusted time	M	4.4.1
SignatureTimeStamp	O	6.1.1
Time Mark or other method	O	4.4.1

6.6 CAdES-A profile

6.6.1 General

The required levels of constituent elements of CAdES-T data are specified in 6.6.2 to 6.6.4.

6.6.2 Structure of the CAdES-A profile

The CAdES-A profile is defined as an extended form of the CAdES-T profile to which the unsigned attributes specified in Table 6 are added. The required level of each element of the portion corresponding to CAdES-T shall be as specified in 6.5.

6.6.3 Additional unsigned attributes

The required level of each element added to unsigned attributes shall be as stated in Table 6. The required level shall be “Conditional” for any element not specified in Table 6.

Table 6 — Additional Unsigned Attributes

Element	Required level	ETSI TS 101 733 v1.8.1 Reference
CompleteCertificateReferences	M	6.2.1
CompleteRevocationReferences	M	6.2.2
CompleteRevRefs CRL	O	6.2.2
CompleteRevRefs OCSP	O	6.2.2
OtherRevRefs	C	6.2.2
Attribute certificate references	C	6.2.3
Attribute revocation references	C	6.2.4
CertificateValues	M	6.3.3
CertificateValues	O	6.3.3
Certificates maintained by trusted service	C	[a]
RevocationValues	M	6.3.4
CertificateList	O	6.3.4
BasicOCSPResponse	O	6.3.4
OtherRevVals	C	6.3.4
Certificates maintained by trusted service	C	[a]
CAdES-C-timestamp	C	6.3.5
Timestamped cert and crls reference	C	6.3.6
Archiving	M	6.4
ArchiveTimestamp id-aa-48	O	6.4.1
ArchiveTimestamp id-aa-27	O	[b]
Evidence Record	O	[c]
Other method	C	[d]

[a] If a certification authority (CA) or other trusted service is trusted to maintain certificates for the archiving period there is no need to hold them with the signature. Instead of this element for the interoperability reasons and to prevent the signature to contain multiple values of the same large CRLs or certificates and OCSPs the elements defined in CMS (Table 2) CertificateSet or RevocationInfoChoices can be used. The OtherRevocationInfoFormat is used for Basic OCSP Response responses.

[b] Defined in ETSI TSA 101 733 v1.4.0 or earlier versions.

[c] Defined in IETF RFC 4998.

[d] If the other trusted service is trusted to maintain timestamping for the archiving period it can be applied.

6.7 Timestamp validation data

The validation of past timestamps requires certificates and revocation information up to the trust anchor. Timestamp validation data requires certificates in the certificate chain from TSA certificates to trust anchor certificates, and the revocation information pertaining to each such certificate.

Validation data may be stored with CAdES-A data as described below. When not stored with CAdES-A data, validation data shall be stored by another secure means including, but not limited to, storage by CA as a TTP or by TSA.

In past timestamp validation, validation data stored as described below or by another secure means may also be used.

Annex B specifies the requirements relevant to the structure of a timestamp token.

a) Validation data for signature timestamp shall be stored upon generation at one of the places set forth below or by CA, etc.

   1) The following elements within unsigned attributes:

      — CertificateValues

— RevocationValues

2) The following elements within the timestamp token in the signature timestamp (signature timestamp token):

— CertificateSet

— RevocationInfoChoices

3) The following elements within the unsigned attributes of the signature timestamp token:

— CertificateValues

— RevocationValues

NOTE The elements under 1) and 2) above are defined in CMS, and those under 3) above in CAdES.

b) Archive timestamp validation data shall be stored upon generation at one of the places set forth below or by CA, etc.

1) The following elements within the timestamp token in the archive timestamp (archive timestamp token):

— CertificateSet

— RevocationInfoChoices

2) The following elements within the unsigned attributes of the archive timestamp token:

— CertificateValues

— RevocationValues

NOTE The elements under 1) above are defined in CMS, and those under 2) above in CAdES.

Annex A
(normative)

Supplier's declaration of conformity and its attachment

A.1 General

This annex sets forth the form of the supplier's declaration of conformity to the CAdES long term signature profile.

A.2 Form of the supplier's declaration of conformity

Supplier's declaration of conformity to the long term signature profile

No. ____________________

Issuer's name: ____

Issuer's address: ____

Object of declaration:

The object of the declaration described above is in conformity with the requirement of the following long term signature profiles.

CAdES-T profile and/or **CAdES-A profile**

The implemented elements are as specified in A.3 below.

Additional information:

(The results of operation checks, etc. may be inserted here.)

Signed for and on behalf of:

____

____

(Place and date of issue)

____

(Name, title)

A.3 Form of the attachment to the supplier's declaration of conformity

A.3.1 General

The attachment to the supplier's declaration of conformity shall contain the items specified in A.3.2 to A.3.7.

A.3.2 Version number of ETSI TS 101 733 to be referenced

A.3.3 Scope of profile implementation

Table A.1 — Profile implementation

Profile identifier	Generator	Verifier
CAdES-T		
CAdES-A		

A.3.4 Conformity to the CAdES-T profile

Table A.2 — Signed data

Element	Required level	Generator	Verifier
CMSVersion	M		
DigestAlgorithmIdentifiers	M		
EncapsulatedContentInfo	M		
eContentType	M		
eContent	O		
CertificateSet (Certificates)	O		
Certificate	O		
AttributeCertificateV2	C		
OtherCertificateFormat	C		
RevocationInfoChoices (crls)	O		
CertificateList	O		
OtherRevocationInfoFormat	C		
SignerInfos	M		
single	O		
parallel	O		

Table A.3 — Signer Info

Element	Required level	Generator	Verifier
CMSVersion	M		
SignerIdentifier	M		
IssuerAndSerialNumber	O		
SubjectKeyIdentifier	O		
DigestAlgorithmIdentifier	M		
SignedAttributes	M		
SignatureAlgorithmIdentifier	M		
SignatureValue	M		
UnsignedAttributes	M		

Table A.4 — Signed attributes

Element	Required level	Generator	Verifier
ContentType	M		
MessageDigest	M		
SigningCertificateReference	M		
ESS SigningCertificate	O		
ESS SigningCertificate v2	O		
OtherSigningCertificate	C		
SignaturePolicyIdentifier	C		
SigningTime	O		
ContentReference	C		
ContentIdentifier	C		
ContentHints	C		
CommitmentTypeIndication	C		
SignerLocation	C		
SignerAttribute	C		
ContentTimestamp	C		

Table A.5 — Unsigned attributes

Element	Required level	Generator	Verifier
CounterSignature	O		
Trusted signing time	M		
SignatureTimeStamp	O		
Time Mark or other method	O		

A.3.5 Conformity to the CAdES-A profile

Table A.6 — Additional unsigned attributes

Element	Required level	Generator	Verifier
CompleteCertificateReferences	M		
CompleteRevocationReferences	M		
CompleteRevRefs CRL	O		
CompleteRevRefs OCSP	O		
OtherRevRefs	C		
Attribute certificate references	C		
Attribute revocation references	C		
CertificateValues	M		
CertificateValues	O		
Certificates maintained by trusted service	C		
RevocationValues	M		
CertificateList	O		
BasicOCSPResponse	O		
OtherRevVals	C		
Certificates maintained by trusted service	C		
CAdES-C-timestamp	C		
Timestamped cert and crls reference	C		
Archiving	M		
ArchiveTimestamp id-aa-48	O		
ArchiveTimestamp id-aa-27	O		
Evidence Record	O		
Other method	C		

A.3.6 Specifications to be referenced by elements "Conditional"

No.	Element name	Referenced specification
1		
2		

NOTE Tables A.2 to A.6 give the names of elements identified as "Conditional" and the referenced specifications.

A.3.7 Remarks
