INTERNATIONAL STANDARD

ISO 14533-1

Second edition
2014-12-01

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 14533-1:2014(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 .... **iv**

Introduction .... **v**

1 Scope **1**

2 Normative references **1**

3 Terms and definitions **1**

4 Symbols **4**

5 Requirements **4**

6 Long term signature profiles **4**

6.1 Defined profiles 4

6.2 Representation of the required level 5

6.3 Standard for setting the required level 5

6.4 Action to take when an optional element is not implemented 6

6.5 CAdES-T profile 6

6.6 CAdES-A profile 8

6.7 Timestamp validation data 10

Annex A (normative) **Supplier's declaration of conformity and its attachment** **12**

Annex B (normative) **Structure of timestamp token** **17**

Bibliography **19**

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, industry and administration*.

This second edition cancels and replaces the first edition (ISO 14533-1:2012), which has been technically revised. The main changes compared with the previous edition are that Clause 6 and Annexes A and B have been technically revised with the addition of a new archive time-stamp format: archive-time-stamp-v3 (ATSv3) and an associated attribute ats-hash-index.

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)*

The following part is under preparation:

— *Part 3: Long term signature profiles for PDF Advanced Electronic Signatures (PAdES)*

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 documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. 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 v2.2.1 (2013-04), *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 1 to entry: 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 1 to entry: 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 1 to entry: 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 1 to entry: 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
- P: Prohibited (creation or modification)

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 If 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.

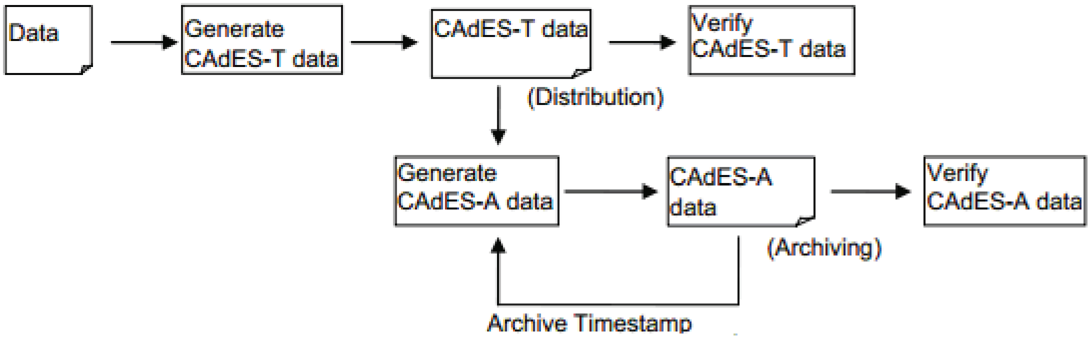

Figure 1 — Relation between CAdES-T data and CAdES-A data

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.

d) Prohibited (P): Elements whose required level is 'Prohibited' shall not be created or modified, may be read.

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 1 OtherCertificateFormat.

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

EXAMPLE 2 ContentReference.

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

EXAMPLE 3 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.

If a certification authority (CA) or other trusted service is trusted to maintain and keep certificates for the signature validation accessible for an appropriate period of time and parties relying on the signature validity know the location where the certificates are accessible, there is no need to hold them with the signature. Otherwise, for the interoperability reasons, the generator should include the signer certificate in CAdES-T. The fields where the signer certificate or validation data may be included are determined according to strategies defined in ETSI/TS 101 733 v2.2.1, 6.4.3, where 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 should be used for BasicOCSPResponse responses (see IETF RFC 6960, 4.2.1).

NOTE The signer certificate is the starting point where the public key for signature verification is stored and contains references where the validation data and issuer certificate are located (see "Authority Information Access" where id-ad-caIssuers and id-ad-ocsp are defined in IETF RFC 5280, 4.2.2.1; and "CRL Distribution Points" where id-ce-cRLDistributionPoints is defined in IETF RFC 5280, 4.2.1.13).

6.5.2 Content information

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

Table 1 — Content information (CAdES-T)

Element	Required level	Value	ETSI/TS 101 733 v2.2.1 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 (CAdES-T)

Element	Required level	ETSI/TS 101 733 v2.2.1 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	O	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 (CAdES-T)

Element	Required level	ETSI/TS 101 733 v2.2.1 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.

Table 4 — Signed Attributes (CAdES-T)

Attribute	Required level	ETSI/TS 101 733 v2.2.1 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 (CAdES-T)

Attribute	Required level	ETSI/TS 101 733 v2.2.1 Reference
CounterSignature	O	5.9.2
Trusted time	M	4.4.1
SignatureTimeStamp	O	6.1.1
Time Mark or other method like archive time-stamp as its replacement	O	4.4.1

6.6 CAdES-A profile

6.6.1 General

The required levels of constituent elements of CAdES-A data are specified in 6.6.2 to 6.6.3.

The required levels of elements differ whether the signature applies the ArchiveTimeStampV3 form; or it applies one of the ArchiveTimeStampV1, ArchiveTimeStampV2 forms.

NOTE The ArchiveTimeStampV1, the ArchiveTimeStampV2, or the long-term-validation forms were defined with the following limitations:

— The hash calculation is invalidated after modification of the CertificateSet element, the RevocationInfoChoices element, the CertificateValues attribute, or the RevocationValues attribute of the time-stamped signature after applying those types of the time-stamp.

— The hash calculation is invalidated when any other unsigned attributes are included after applying those types of the time-stamp.

— The hash calculation can be invalidated according to usage of different incompatible implementations where BER or DER reordering (see ISO/IEC 8825-1:2008, 11.6) is used or where the tag and the length of unsigned attributes SET OF are included or not in the archive time-stamp hashing procedure.

— CMS implementations are not able to use certificates or revocation values stored in unsigned attributes CertificateValues or RevocationValues. A usage of such unsigned attributes causes a redundant presence of multiple values in parallel signatures or in any types of time-stamps.

Creation of the ArchiveTimeStampV1, ArchiveTimeStampV2, or long-term-validation forms were deprecated in ETSI/TS 101 733 v2.2.1. ArchiveTimeStampV3 should be used for a new archive time-stamp.

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 — Unsigned Attributes (CAdES-A)

Attribute	Required level		ETSI/TS 101 733 v2.2.1
	ArchiveTimeStampV3	ArchiveTimeStampV1/V2	Reference
CounterSignature	C	C[e]	5.9.2
Trusted time	M	M	4.4.1
SignatureTimeStamp	O	O	6.1.1
Time Mark or other method like archive time-stamp as its replacement	O	O	4.4.1
CompleteCertificateReferences	C	M[e]	6.2.1
CompleteRevocationReferences	C	M[e]	6.2.2
CompleteRevRefs CRL	O	O	6.2.2
CompleteRevRefs OCSP	O	O	6.2.2
OtherRevRefs	C	C	6.2.2
Attribute certificate references	C	C[e]	6.2.3
Attribute revocation references	C	C[e]	6.2.4
CertificateValues	C	M[e]	6.3.3
CertificateValues	O	O	6.3.3
Certificates maintained by trusted service	C	C	[a]
RevocationValues	C	M[e]	6.3.4
CertificateList	O	O	6.3.4
BasicOCSPResponse	O	O	6.3.4
OtherRevVals	C	C	6.3.4
RevocationValues maintained by trusted service	C	C	[a]
CAdES-C-timestamp	C	C	6.3.5
Timestamped cert and crls reference	C	C	6.3.6
Archiving	M	M	6.4
ArchiveTimestampV3 id-aa-ets-archiveTimestampV3	O	O	6.4.3
ArchiveTimestampV2 ArchiveTimestamp id-aa-48	C[f]	O	6.4.1
ArchiveTimestampV1 ArchiveTimestamp id-aa-27	C[f]	O	[b]
Evidence Record	O	O	[c]
Other method	C	C	[d]

[a] If a certification authority (CA) or other trusted service is trusted to maintain and keep the signature validation data accessible for an appropriate period of time and parties relaying on the signature validity know the location where the signature validation data are accessible, there is no need to hold them with the signature.

[b] Defined in ETSI/TS 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.

[e] Attribute shall not be included after applying those types of the time-stamp.

[f] Not recommended attribute.

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.

Validation data for signature time-stamp shall be stored upon generation at one of the places specified in Table 7 or by CA, etc. The elements of storing validation data differ whether the signature applies the ArchiveTimeStampV3 form; or it applies one of the ArchiveTimeStampV1, ArchiveTimeStampV2 forms as shown in Table 7.

Table 7 — Elements of storing validation data for signature time-stamp

Elements of storing validation data		**ArchiveTimeStampV3**		**ArchiveTimeStampV1/V2**	
		Required level	**Preferred order**	**Required level**	**Preferred order**
SignedData of time-stamped signature	CertificateSet	O	2	O	2
	RevocationInfoChoices	O	1	O	2
	CertificateValues attribute	C[a]		O	3
	RevocationValues attribute	C[a]		O	3
Timestamp token of the signature timestamp	CertificateSet	O	1	O	1
	RevocationInfoChoices	O	2	O	1
	CertificateValues attribute	C[a]		O	4
	RevocationValues attribute	C[a]		O	4

[a] Not recommended attribute.

Archive timestamp validation data shall be stored upon generation at one of the places specified in Table 8 or by CA, etc. The elements of storing validation data differ whether the signature applies the ArchiveTimeStampV3 form; or it applies one of the ArchiveTimeStampV1, ArchiveTimeStampV2 forms as shown in Table 8.

Table 8 — Elements of storing validation data for archive time-stamp

Elements of storing validation data		**ArchiveTimeStampV3**		**ArchiveTimeStampV1/V2**	
		Required level	**Preferred order**	**Required level**	**Preferred order**
SignedData of archive time-stamped signature	CertificateSet	O	2	P	
	RevocationInfoChoices	O	1	P	
	CertificateValues attribute	P		P	
	RevocationValues attribute	P		P	
Timestamp token of the archive timestamp	CertificateSet	O	1	O	1
	RevocationInfoChoices	O	2	O	1
	CertificateValues attribute	C[a]		O	2
	RevocationValues attribute	C[a]		O	2

[a] Not recommended attribute.

Annex A
(normative)

Supplier’s declaration of conformity and its attachment

A.1 General

This annex specifies 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 Clause A.3.

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 (CAdES-T)

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

Table A.3 — Signer Info (CAdES-T)

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 (CAdES-T)

Attribute	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 (CAdES-T)

Attribute	Required level	Generator	Verifier
CounterSignature	C		
Trusted signing time	M		
SignatureTimeStamp	O		
Time Mark or other method like archive time-stamp as its replacement	O		

A.3.5 Conformity to the CAdES-A profile

Table A.6 — Unsigned Attributes (CAdES-A)

Attribute	Required level		Generator	Verifier
	ArchiveTimeStampV3	ArchiveTimeStampV1/V2		
CounterSignature	C	C[a]		
Trusted time	M	M		
SignatureTimeStamp	O	O		
Time Mark or other method like archive time-stamp as its replacement	O	O		
CompleteCertificateReferences	C	M[a]		
CompleteRevocationReferences	C	M[a]		
CompleteRevRefs CRL	O	O		
CompleteRevRefs OCSP	O	O		
OtherRevRefs	C	C		
Attribute certificate references	C	C[a]		
Attribute revocation references	C	C[a]		
CertificateValues	C	M[a]		
CertificateValues	O	O		
Certificates maintained by trusted service	C	C		
RevocationValues	C	M[a]		
CertificateList	O	O		
BasicOCSPResponse	O	O		
OtherRevVals	C	C		
Certificates maintained by trusted service	C	C		
CAdES-C-timestamp	C	C		
Timestamped cert and crls reference	C	C		
Archiving	M	M		
ArchiveTimestampV3 id-aa-ets-archiveTimestampV3	O	O		
ArchiveTimestampV2 ArchiveTimestamp id-aa-48	C[b]	O		
ArchiveTimestampV1 ArchiveTimestamp id-aa-27	C[b]	O		
Evidence Record	O	O		
Other method	C	C		

[a] Attribute shall not be included after applying those types of the time-stamp.

[b] Not recommended attribute.

A.3.6 Specifications to be referenced by elements “Conditional”

Table A.7 — "Conditional" elements

No.	Element name	Referenced specification
1.	OtherRevocationInfoFormat	id-pkix-ocsp-basic of BasicOCSPResponse in IETF RFC 6960, 4.2.1
2.	OtherRevocationInfoFormat	id-ri-ocsp-response of OCSPResponse in IETF RFC 5940, Clause 3, and in IETF RFC 6960, 4.2.1
3.	CounterSignature, CompleteCertificateReferences, CompleteRevocationReferences, Attribute certificate references, Attribute revocation references, CertificateValues, RevocationValues, CAdES-C-timestamp, Timestamped cert and crls reference, ArchiveTimestampV2 and ArchiveTimestampV1	When ArchiveTimeStampV3 is applied, while ArchiveTimeStampV1 or ArchiveTimeStampV2 is included in signature or in any parallel signatures, then conditions defined for ArchiveTimeStampV1 or ArchiveTimeStampV2 are used for enumerated elements otherwise enumerated elements are used as optional (O). See ETSI/TS 101 733 v2.2.1, 4.4.4 and 6.4.

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

A.3.7 Remarks

Annex B
(normative)

Structure of timestamp token

B.1 General

This annex specifies the requirements for the structure of a timestamp token in a long term signature.

B.2 Normative specifications

The signature timestamp token and archive timestamp token in this part of ISO 14533 shall conform to CMS, TSP and CAdES.

NOTE Time-Stamp Protocol (TSP) is defined in IETF RFC 3161.

B.3 Required level of constituent elements

The required level of each element of the signature timestamp token and archive timestamp token shall be as specified in Table B.1. The required levels of elements differ whether the signature applies the ArchiveTimeStampV3 form; or it applies one of the ArchiveTimeStampV1, ArchiveTimeStampV2 forms.

Table B.1 — Required level of each element of the timestamp token

Element	Required level		Value
	ArchiveTimeStampV3	ArchiveTimeStampV1/V2	
ContentType	M	M	id-signedData
Content	M	M	Signed Data
CMSVersion	M	M	
DigestAlgorithmIdentifiers	M	M	
EncapsulatedContentInfo	M	M	
eContentType	M	M	id-ct-TSTInfo
eContent	M	M	DER-encoded value of TSTInfo
CertificateSet (Certificates)	O[a]	O[a]	
Certificate	O	O	
AttributeCertificateV1	O	O	
AttributeCertificateV2	O	O	
OtherCertificateFormat	O	O	
RevocationInfoChoices (crls)	O	O	
CertificateList	O	O	
OtherRevocationInfoFormat	O	O	
SignerInfos	M	M	
SignerInfo	M	M	
CMSVersion	M	M	
SignerIdentifier	M	M	

[a] The generator includes the signer certificate, if the certReq field is present and set to true, according to IETF RFC 3161, 2.4.1, updated with IETF RFC 5816.

Table B.1 *(continued)*

Element	Required level		Value
	ArchiveTimeStampV3	ArchiveTimeStampV1/V2	
IssuerAndSerialNumber	O	O	
SubjectKeyIdentifier	O	O	
DigestAlgorithmIdentifier	M	M	
SignedAttributes	M	M	
ContentType	M	M	id-ct-TSTInfo
MessageDigest	M	M	
SigningCertificateReference	M	M	
ESS SigningCertificate	O	O	
ESS SigningCertificate v2	O	O	
OtherSigningCertificate	C	C	
SignatureAlgorithmIdentifier	M	M	
SignatureValue	M	M	
UnsignedAttributes	M	O	
ATSHashIndex	M	C	id-aa-ATSHashIndex
CompleteCertificateReferences	C	O	
CompleteRevocationReferences	C	O	
CompleteRevRefs CRL	O	O	
CompleteRevRefs OCSP	O	O	
CertificateValues	C	O	
CertificateValues	O	O	
Storage of the certificate by CA	C	C	
RevocationValues	C	O	
CertificateList	O	O	
BasicOCSPResponse	O	O	

[a] The generator includes the signer certificate, if the certReq field is present and set to true, according to IETF RFC 3161, 2.4.1, updated with IETF RFC 5816.

Bibliography

[1] ISO/IEC 8825-1:2008, *Information technology — ASN.1 encoding rules — Part 1: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)*

[2] ISO/IEC 9594-8, *Information technology — Open Systems Interconnection — The Directory — Part 8: Public-key and attribute certificate frameworks*

[3] ISO/IEC 18014-2, *Information technology — Security techniques — Time-stamping services — Part 2: Mechanisms producing independent tokens*

[4] IETF RFC 3161, *Time-Stamp Protocol (TSP)*

[5] IETF RFC 4998, *Evidence Record Syntax (ERS)*

[6] IETF RFC 5280, *Internet X.509 Public Key Infrastructure, Certificate and Certificate Revocation List (CRL) Profile*

[7] IETF RFC 5652, *Cryptographic Message Syntax (CMS)*[2)]

[8] IETF RFC 5816, *ESSCertIDv2 Update for RFC 3161*

[9] IETF RFC 5940, *Additional Cryptographic Message Syntax (CMS) Revocation Information Choices*

[10] IETF RFC 6960, *Online Certificate Status Protocol (OCSP)*

[2)] Available from <http://www.ietf.org/>

ICS 35.240.60

Price based on 19 pages