
**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)**

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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

ISO 14533-1:2012

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

<https://standards.iteh.ai/catalog/standards/sist/62191530-cc23-928-9106-d509455900/iso-14533-1-2012>



iTeh STANDARD PREVIEW (standards.iteh.ai)

ISO 14533-1:2012

<https://standards.iteh.ai/catalog/standards/sist/8a15f386-ce23-452d-910b-d5c09453905c/iso-14533-1-2012>



COPYRIGHT PROTECTED DOCUMENT

© ISO 2012

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

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	3
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	5
6.5 CAdES-T profile	6
6.6 CAdES-A profile	7
6.7 Timestamp validation data	8
Annex A (normative) Supplier's declaration of conformity and its attachment	10
Annex B (normative) Structure of timestamp token	14
Bibliography	16

ITeh STANDARD PREVIEW
(standards.iteh.ai)

[ISO 14533-1:2012](https://standards.iteh.ai/catalog/standards/sist/8a15f386-ce23-452d-910b-d5c09453905c/iso-14533-1-2012)

<https://standards.iteh.ai/catalog/standards/sist/8a15f386-ce23-452d-910b-d5c09453905c/iso-14533-1-2012>

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 (CAAdES)
- Part 2: Long term signature profiles for XML Advanced Electronic Signatures (XAdES)

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[ISO 14533-1:2012](https://standards.iteh.ai/catalog/standards/sist/8a15f386-ce23-452d-910b-d5c09453905c/iso-14533-1-2012)

<https://standards.iteh.ai/catalog/standards/sist/8a15f386-ce23-452d-910b-d5c09453905c/iso-14533-1-2012>

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 (CAAdES) developed by the European Telecommunications Standards Institute (ETSI).

iTeh STANDARD PREVIEW (standards.iteh.ai)

[ISO 14533-1:2012](https://standards.iteh.ai/catalog/standards/sist/8a15f386-ce23-452d-910b-d5c09453905c/iso-14533-1-2012)

<https://standards.iteh.ai/catalog/standards/sist/8a15f386-ce23-452d-910b-d5c09453905c/iso-14533-1-2012>

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO 14533-1:2012

<https://standards.iteh.ai/catalog/standards/sist/8a15f386-ce23-452d-910b-d5c09453905c/iso-14533-1-2012>

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 (CAAdES)

1 Scope

This part of ISO 14533 specifies the elements, among those defined in CMS Advanced Electronic Signatures (CAAdES), 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 (CAAdES) 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 (CAAdES)*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
CAAdES

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

3.6
CAAdES with time
CAAdES-T

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

EXAMPLE Signature timestamp.

3.7
archival CAAdES
CAAdES-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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

3.8
content information

data structure that defines the content in CMS

[ISO 14533-1:2012](https://standards.iteh.ai/catalog/standards/sist/8a15f386-ce23-452d-910b-d5c09453905c/iso-14533-1-2012)

<https://standards.iteh.ai/catalog/standards/sist/8a15f386-ce23-452d-910b-d5c09453905c/iso-14533-1-2012>

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.

<https://standards.iteh.ai/catalog/standards/sist/8a15f386-ce23-452d-910b-d5c09453905c/iso-14533-1-2012>

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 revoked 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

ISO 14533-1:2012
<http://standards.iteh.ai/catalog/standards/sist/8a15f386-ce23-452d-910b-d5c09453905c/iso-14533-1-2012>

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.

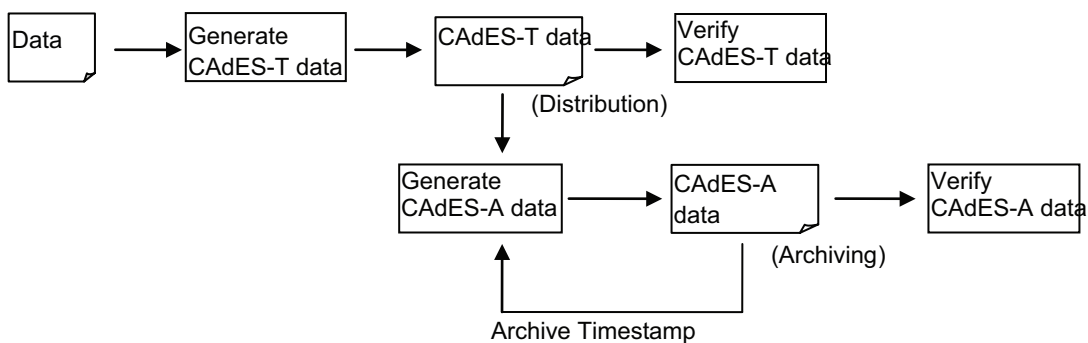


Figure 1 — Relation between CADES-T data and CADES-A data

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 <https://standards.iteh.ai/catalog/standards/sist/8a15f386-ce23-452d-910b-d5c09453905c/iso-14533-1-2012>
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.