INTERNATIONAL STANDARD

ISO 14533-1

Third edition
2022-06

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

Part 1: Profiles for CMS Advanced Electronic Signatures (CAdES)

Reference number
ISO 14533-1:2022(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: 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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 154 *Processes, data elements and documents in commerce, industry and administration*.

This third edition cancels and replaces the second edition (ISO 14533-1:2014), which has been technically revised.

The main changes are as follows:

— Clause 6 and Annex 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-v3 and with the addition of other methods defined in ISO 14533-4:2019.

A list of all parts in the ISO 14533 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user’s national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

The purpose of this document is to ensure the interoperability of implementations with respect to long term signatures that make digital signatures verifiable for a long term. Long term signature specifications referenced by each implementation cover Cryptographic Message Syntax (CMS) digital signatures defined in IETF RFC 5652 extended in CAdES digital signatures developed by the European Telecommunications Standards Institute (ETSI).

ETSI changes 'CMS Advanced Electronic Signature' to 'CAdES Digital Signature' from TS to EN. In this document, CAdES is used also in line with the ETSI EN definition.

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

Part 1: Profiles for CMS Advanced Electronic Signatures (CAdES)

1 Scope

This document specifies the elements, among those defined in CMS digital signatures and CAdES digital signatures 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 CAdES digital signature is the extended specification of Cryptographic message syntax (CMS), used widely.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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.

ISO 14533-4, *Processes, data elements and documents in commerce, industry and administration — Long term signature profiles — Part 4: Attributes pointing to (external) proof of existence objects used in long term signature formats (PoEAttributes)*

3 Terms and definitions

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

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
long term signature
signature that is made verifiable having the ability to maintain its validity status and to get a proof of existence of the associated signed data 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

3.3
required level
level of requirement for implementing each element constituting a *profile* (3.2)

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 digital signature
CAdES digital signature
CAdES
digital signature for which the signer can be identified, and any illegal data alteration detected

Note 1 to entry: Note 1to entry: A digital signature is defined in IETF/RFC 5652 and ETSI/EN 319 122-1.

3.6
CAdES-T
CAdES with time
CAdES digital signature with information to ascertain signing time

EXAMPLE Signature time-stamp.

Note 1 to entry: A CAdES digital signature is defined in ETSI/EN 319 122-1.

3.7
CAdES-A
archival CAdES
CAdES digital signature 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 time-stamp.

Note 1 to entry: A CAdES digital signature is defined in ETSI/EN 319 122-1.

3.8
content information
data structure that defines the content in CMS

3.9
signed data
data structure 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 time-stamp and archive time-stamp are unsigned attributes.

3.13
validation data
certificate and revocation information used to validate a signature and time-stamp

3.14
time-stamping authority
TSA
trusted third party (3.19) commissioned to provide proof that certain data existed prior to a certain point in time

3.15
time-stamp 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 time-stamp
time-stamp affixed to a signature value in order to identify the time when the signature existed

3.17
archive time-stamp
time-stamp affixed to information pertaining to a signature, including the subject of the signature and *validation data* (3.13), 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, see ISO/IEC 9594-8.

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* (3.20) to prevent forgery

3.22
attribute certificate
certificate (3.21) containing the job, qualification, position, and other attributes and attribute values

3.23
revocation information
information issued by a *certification authority* (3.20) 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 document 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 document, 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 document, shall be provided.

5.2 The generation or validation of CAdES-A data conforms to this document 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 document, 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 document, shall be provided.

5.3 If first-party conformity assessment is used, the implementer shall make a declaration of conformity to this document by disclosing the supplier's declaration of compliance and its attachment (as given in Annex A) containing a description of implementation status (and the specifications for any “Conditional” elements).

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 document 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.

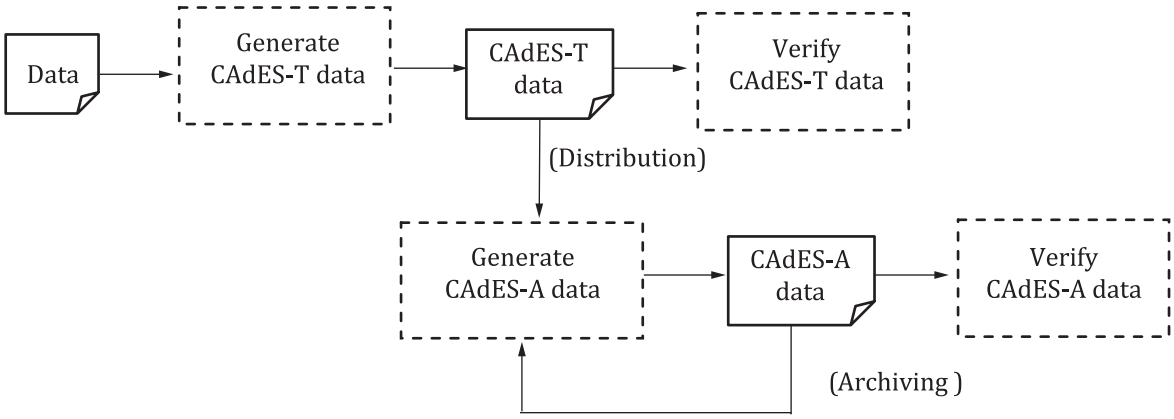

Figure 1 — Relation between CAdES-T data and CAdES-A data

6.2 Representation of the required level

This document 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 sub-elements, at least one sub-element shall be selected. Any element whose required level is "Mandatory" and is one of the sub-elements 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 CMSAlgorithmProtection attribute (IETF RFC 6211) as one of the signed attributes, see IETF RFC 8933.

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, e.g. as specified in ISO 14533-4.