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)