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

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