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

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

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

*Partie 3: Profils de signature à long terme pour les signatures
électroniques avancées PDF (PAdES)*





COPYRIGHT PROTECTED DOCUMENT

© ISO 2017, Published in Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

Foreword	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Abbreviated terms and symbols	1
5 Requirements	2
6 Long-term signature profiles	2
6.1 Definition of PAdES profile and positioning	2
6.2 Representation of the required level	3
6.3 Standard for setting the required level	3
6.4 PAdES-T profile	4
6.4.1 General	4
6.4.2 PAdES using CAdES signatures profile	5
6.4.3 Timestamp of PAdES-T profile	8
6.5 PAdES-A profile	8
6.5.1 General	8
6.5.2 Structure of the PAdES-A profile	8
6.5.3 Document Security Store Dictionary	9
6.5.4 Signature VRI Dictionary	9
6.5.5 Document timestamp	9
6.5.6 Updating PAdES-A	10
6.5.7 Validation Data for Signature and Timestamp	10
6.6 Multiple signatures	10
6.6.1 General	10
6.6.2 Timestamp for multiple signatures	11
Annex A (normative) Supplier's declaration of conformity and its attachment	13
Annex B (normative) The profile for using only timestamp	18
Annex C (normative) Structure of timestamp token	20
Annex D (informative) Applying PAdES using CMS signatures	22
Annex E (informative) Examples of multiple signatures	23
Bibliography	26

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 on 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 the following URL: 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*.

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

Introduction

The purpose of this document is to ensure the interoperability of implementations with respect to long-term signatures that make electronic signatures verifiable in the long term. Long-term signature specifications referenced by each implementation cover PDF Advanced Electronic Signatures (PAdES) developed by the European Telecommunications Standards Institute (ETSI).

