ISO 14533-3:2017-09 (E)

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)

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