ISO 14533-4:2019-08 (E)

Processes, data elements and do cuments 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)

Contents

Page

Foreword iv

Introduction v

1 Scope 1

2 Normative references 1

3 Terms and definitions 2

4 PoE attributes 4
4.1 General concept of PoE 4
4.2 Abstract attribute PoEAttribute 5
4.3 LTI PoEAttribute instance based on IETF RFC 3161 timestamp or IETF RFC 4998/ IETF RFC 6283 evidence record 8
4.4 ERS PoEAttribute instance based on IETF RFC 4998/IETF RFC 6283 evidence record 12
4.5 TStOCSP PoEAttribute instance 12
4.6 Attribute PoEHashIndex 13
4.7 Attribute preservation-integrity-list 14

5 Types of PoE objects with their essential fields 16
5.1 General 16
5.2 PoE object of status at thisUpdate time value based on CertHash OCSP SingleResponse extension 17
5.3 PoE object supported by LTI PoEAttribute or ERS PoEAttribute 18

Annex A (normative) ASN.1 module 19

Annex B (normative) Definition of the CertHash OCSP SingleResponse extension 20

Annex C (normative) Signature timestamp as a timestamp through OCSP 21

Annex D (normative) Syntax of the ASN.1 object location in ZIP, PDF container or in DER encoded ASN.1 object 23

Annex E (normative) Use of the PoE objects 26

Annex F (informative) Location of DTId in the digital signature 32

Annex G (informative) Media type registrations 33

Annex H (informative) Evidence record syntax object 34

Bibliography 36