
**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)**

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

*Partie 4: Attributs pointant vers des objets externes de la Preuve de
l'existence utilisés dans les formats de la signature à long terme*

<https://standards.iteh.ai/catalog/standards/iso/7268a285-8366-4bb5-9506-b6de219964bb/iso-14533-4-2019>



iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

ISO 14533-4:2019

<https://standards.iteh.ai/catalog/standards/iso/7268a285-856b-4bb3-9506-b6de2f9964bb/iso-14533-4-2019>



COPYRIGHT PROTECTED DOCUMENT

© ISO 2019

All rights reserved. Unless otherwise specified, or required in the context of its implementation, 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
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

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 <i>PoEAttribute</i> instance based on IETF RFC 3161 timestamp or IETF RFC 4998/ IETF RFC 6283 evidence record	8
4.4 ERS <i>PoEAttribute</i> instance based on IETF RFC 4998/IETF RFC 6283 evidence record	12
4.5 TStOCSP <i>PoEAttribute</i> 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 <i>thisUpdate</i> time value based on <i>CertHash</i> OCSP <i>SingleResponse</i> 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 <i>CertHash</i> OCSP <i>SingleResponse</i> 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

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*.

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

This document provides detailed information associated with the analysis, selection and implementation of procedures associated with long term signatures. The development of this document is a result of organizational requests to receive information of already existing objects defined in technology standards, technical reports, and industry best practices for electronic signatures verifiable for a long term.

The purpose of this document is to ensure the interoperability of implementations with respect to long term signatures that make electronic signatures verifiable for a long term. This document clarifies conditions used in the validation procedure to provide a complete and unalterable result.

iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

[ISO 14533-4:2019](https://standards.iteh.ai/catalog/standards/iso/7268a285-856b-4bb3-9506-b6de2f9964bb/iso-14533-4-2019)

<https://standards.iteh.ai/catalog/standards/iso/7268a285-856b-4bb3-9506-b6de2f9964bb/iso-14533-4-2019>

