INTERNATIONAL STANDARD

ISO 14533-4

First edition
2019-08

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

Reference number
ISO 14533-4:2019(E)

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

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.

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)

IMPORTANT — The electronic file of this document contains colours which are considered to be useful for the correct understanding of the document. Users should therefore consider printing this document using a colour printer.

1 Scope

This document specifies the elements defined in the international standards of ISO/ITU-T, ETSI and IETF RFC that enable at least a proof of existence of data objects and digital signatures and the preservation of the validity status of digital signatures over a long period of time used in validation.

It provides the definitions of the proof of existence (PoE) attributes and clarification of the usage of (external) PoE objects, with digital signatures and trusted time values, which have already existed and can be used by the PoE attributes pointing to (external) PoE objects used in long term signature validation or preservation.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 8825-1[1)], *Information technology — ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER) — Part 1*

ISO/IEC 9594-8[2)], *Information technology — Open Systems Interconnection — The Directory — Part 8: Public-key and attribute certificate frameworks*

ISO 32000-2, *Document management — Portable document format — Part 2: PDF 2.0*

ETSI EN 319 122-1, V1.1.1:2016-04, *Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures*

IETF RFC 3161[3)], *Timestamp Protocol (TSP)*

IETF RFC 6960[4)], *Online Certificate Status Protocol (OCSP)*

IETF RFC 4648[5)], *The Base16, Base32, and Base64 Data Encodings*

1) Also known as ITU-T Recommendation X.690.

2) Also known as ITU-T Recommendation X.509.

3) Available at https://tools.ietf.org/html/3161.

4) Available at https://tools.ietf.org/html/6960.

5) Available at https://tools.ietf.org/html/4648.

IETF RFC 4998[6], *Evidence Record Syntax (ERS)*

IETF RFC 6283[7], *Extensible Markup Language Evidence Record Syntax (XMLERS)*

IETF RFC 5652[8], *Cryptographic Message Syntax (CMS)*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 9594-8, ISO 32000-2, ISO/IEC 8825-1, IETF RFC 3161, IETF RFC 6960 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1
digital signature
data appended to, or cryptographic transformation of, a data string that proves the origin and the integrity of the data string and protects against forgery, e.g. by the recipient of the data string

Note 1 to entry: Digital signatures in the present document cover also electronic signatures, advanced electronic signatures, qualified electronic signatures, electronic seals, advanced electronic seals, qualified electronic seals, electronic time stamps and qualified electronic time stamps as per Regulation (EU) No 910/2014[6] and ISO/IEC 9594-8 certificate, CRL (see ISO/IEC 9594-8) or OCSP response and signatures defined in profiles ISO 14533-1, ISO 14533-2 or ISO 14533-3.

[SOURCE: ISO/IEC 7816-4:2013, 3.21, modified — Note 1 to entry has been added.]

3.2
document identifier
DId
indirect identifier for machine processing in the form of DER encoded ASN.1 type `MessageImprint` defined in IETF RFC 3161 covering the electronic document

3.3
document signature identifier
DSId
indirect identifier of signature of a document for machine processing in the form of DER encoded ASN.1 type `MessageImprint` defined in IETF RFC 3161 covering the DER encoded result of the asymmetric signature algorithm

EXAMPLE ECDSA or RSA result included in the *digital signature* (3.1) of the signed electronic document.

Note 1 to entry: DSId is mainly used for indirect machine processing identification of the electronic document which is electronically signed, e.g. DSId is used for PDF document identification if PDF file contains many versions of PDF document created by including incremental updates (see ISO 32000-2:2017, 7.5.6 for details) after more than one PDF document timestamps (see ISO 32000-2:2017, 12.8.5) or by including incremental updates after PDF signature or after PDF document timestamp.

Note 2 to entry: Indirect identifier means a relatively unique changeable hash value changing according to the used hash algorithm. A hash collision is when two different input strings of a hash function produce the same hash result.

6) Available at https://tools.ietf.org/html/4998.

7) Available at https://tools.ietf.org/html/6283.

8) Available at https://tools.ietf.org/html/5652.

3.4
document type identifier
DTId
sequence of the characters associated with the electronic document used for determining the format and interpretation of the electronic document

Note 1 to entry: DTId is crucial for correct interpretation of the content of electronic document protected by *digital signature* (3.1). DTId is implemented as the file name extension or the value of the content type (see IETF RFC 2231 or IETF RFC 2045), whose value is included in the fields protected by the digital signature (see Annex F).

3.5
end-of-line marker
EOL marker
sequence of one or two characters marking the end of a line, consisting of a CARRIAGE RETURN character (0Dh) or a LINE FEED character (0Ah) or a CARRIAGE RETURN followed immediately by a LINE FEED

3.6
evidence record
ER
collection of evidence created for one or more given data objects over time, which can be used to prove the integrity and existence of a data object or a data object group at a certain time

Note 1 to entry: See IETF RFC 4998, IETF RFC 6283 and ETSI SR 019 510.

3.7
long term
period of time long enough for there to be concern about the impacts of changing technologies, including support for new media and data formats, and of a changing user community, on the information being held in a repository, which may extend into the indefinite future

Note 1 to entry: Cryptographic algorithms could become weak.

3.8
long-term integrity preservation
long-term preservation
LTI
extension of the validity status of a *digital signature* (3.1) over long periods of time and/or of provision of proofs of existence of data over long periods of time, in spite of the obsolescence of cryptographic technology such as crypto algorithms, key sizes or hash functions, key compromises or of the loss of the ability to check the validity status of public key certificates

3.9
object identifier as a hash
ObjectId
hash reference of the *PoE object* (3.12), *PoE attribute* (3.11) or data object, consisting of object identifier like *DId* (3.2) or *DSId* (3.3)

3.10
proof of existence
PoE
evidence that proves that an object existed at a specific date/time

Note 1 to entry: See ETSI SR 019 510.

3.11
proof of existence attribute
PoE attribute
reference to the *PoE object* (3.12) containing also PoE object type, optional PoE object location, optional storage for the PoE object and optional data object references as additional clarification of data object(s), protected by PoE object, thus unambiguously specifying their semantics

Note 1 to entry: PoE attribute can be a signed or unsigned object of the *digital signature* (3.1) or the file containing the *ObjectId* (3.9), e.g. *DId* (3.2) or *DSId* (3.3), of PoE object. See 4.1 or Annex G, where the type of PoE object is the file name extension like, e.g. "timestampedFile.EXT.TST.DSId" containing PoE object. The file is stored in "timestampedFile.EXT". The timestamp is stored in timestamp file "timestampedFile.EXT.TST".

3.12
proof of existence object
PoE object
property that represents information about a protected data object like type, status or integrity, a trustworthy information of date and time and a *digital signature* (3.1), possibly as part of a timestamp, which proves the integrity of the PoE object and optionally also the origin of the PoE object

Note 1 to entry: See *DId* (3.2) or *DSId* (3.3).

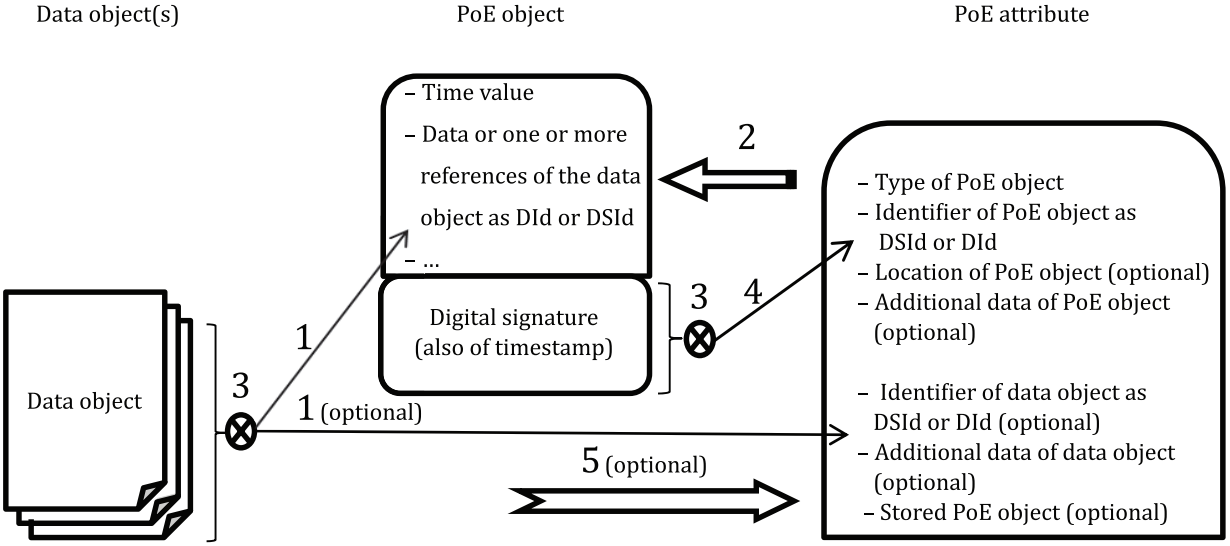
3.13
trusted list
TL
predefined list of items signed by a trusted entity where all the items are authenticated and approved by a trusted signing entity

Note 1 to entry: The primary use of TLs is to verify signed objects, using the TL as a source of trust anchors (see ISO/IEC 9594-8) — trusted root certificates. For more information about the TL see the documentation of operating systems, e.g. Windows, iOS, or the Regulation (EU) No 910/2014[6] (eIDAS Regulation).

4 PoE attributes

4.1 General concept of PoE

This document specifies the PoE attribute as an object which provides a reference between optional data object(s) and the trusted evidence (PoE object) of at least one property of the data object or a set of data objects, especially the integrity, status, type of data object or type of interpretation at a specific time interval or at the date and time, see Figure 1. The PoE attribute is defined in this document as an optional object included in signed attributes or in unsigned attributes as an extension of formats profiled in ISO 14533-1, ISO 14533-3 or marginally in ISO 14533-2 by using elements with similar fields. The PoE attribute is defined also in the form of the file containing ObjectId (e.g. DId or DSId) of the PoE object where the file name of the PoE attribute is the file name of the file containing the PoE object concatenated with a file name extension defined in Annex G, e.g. the data object file is "reports.PNG", the PoE object — file with timestamp is "reports.PNG.TST" and the PoE attribute file is "reports.PNG.TST.DSId".



Key

1 the field where the hash value of the data object is stored
2 referenced PoE object from the PoE attribute
3 hash calculation
4 the field where the hash value of the signature of PoE object is stored
5 PoE object can be stored in the PoE attribute

Figure 1 — PoE concept

The PoE object

— can be external to the data object (two separate objects), called an external PoE object,

— can contain the data object, or

— can be a part of the data object.

NOTE 1 An example of the PoE object, which is a part of the data object, is the PDF document timestamp included in the PDF file where the document timestamp protects one PDF document, usually modified by incremental updates, of many PDF documents included in one PDF file. If the PDF document is protected by the PDF document timestamp or PDF CMS signature, then one DSId can be used for identifying one version of PDF document out of many versions of PDF document included in one PDF file.

NOTE 2 The CMS signed or unsigned attributes, defined in this document, can be used in any form of the CMS signature. When the CMS signature is included in the PDF as the PDF signature (see ISO 32000-2), CMS attributes are modified only before storing the CMS object into the PDF document. A similar functionality can be implemented in the XML digital signature using the *Reference* element, e.g. used in a *Manifest* element (see ISO 14533-2).

4.2 Abstract attribute PoEAttribute

The attribute PoEAttribute is an implementation of the PoE attribute as a DER/JER (see ISO 8825-8) encoded file or as a signed or unsigned attribute of the CMS signature (see Note 1 to entry in 3.11 for other types of implementations) and it is identified by *id-PoEAttribute* OID as specified in Annex A. The attribute PoEAttribute is defined as an abstract incomplete attribute and shall be implemented in derived attributes. It defines the common semantics of the fields which can be used or modified in derived attributes, e.g. in LTI PoE attribute, in ERS PoE attribute, in TStOCSP PoE attribute or in other derived implementations (defined in the future).

The value of *PoEAttribute.poEObjectRef.type* field determines the type of *PoEAttribute* instance and the semantics of the *poEObjectRef* fields (*objectId*, *location*, *additionalData*, *partialHash*, *contentDescription*), of the *poEObject* and of the *dataObjectRefs* fields.

The *poEObjectRef* field of the *PoEAttribute* instance contains:

— The *objectId* field is either of the *DSId* type covering a PoE digital signature (see 3.1) of the (external) PoE object or of the *DId* type covering the whole (external) PoE object.

— The optional *location* field shall be the URL location of the CMS signature, as specified in Annex D, where the PoE object is stored, e.g. location contains "#{DSId-x" where "x" is DSId for identification of one parallel signature or location of ER object storage. See EXAMPLE 2 in Annex D, IETF RFC 8089 or IETF RFC 7230, Section 2.7, where URI is used throughout HTTP as the means for identifying resources or Annex D for additional rules when ASN.1 object is stored in ZIP, PDF container or in another ASN.1 objects. If the optional field *poEObject* is included in the *PoEAttribute* instance, the field *location* should not be included.

— The optional *additionalData* field shall be a storage field for additional data used in creation, in accession or in validation of the PoE object.

— The optional *partialHash* field shall be a storage field for additional hash value used in creation, in accession or in validation of the PoE object.

— The optional *contentDescription* field shall be used for additional information about the PoE object, e.g. *contentDescription* can contain MIME header defined in IETF RFC 2045 (see Annex F).

The optional *poEObject* field of the *PoEAttribute* instance should be a storage of the PoE object in the *PoEAttribute* only if the signature format does not define a field for this type of PoE object. The *poEObject* field should be included only in one signature and only in the *PoEAttribute* instance which supports this PoE object. The *PoEAttribute* instance supports the PoE object if

— the hash algorithm in the *poEObjectRef.objectId* field is the same as used in PoE object, and

— the *PoEAttribute* instance contains the optional *dataObjectRefs* field (if needed) with references to the protected data objects. The optional *dataObjectRefs* field shall be included only in the *PoEAttribute* instance which supports the PoE object to avoid duplication of data or misusing this field.

The other signatures contain only the *PoEAttribute* instance used as a reference to the supporting *PoEAttribute* instance. One *ObjectRef* instance of many instances included in the *dataObjectRefs* field shall contain a reference to the data object with optional clarification of the data object, e.g. provides the type of data object interpretation. The data object is the object of the CMS signature where the *PoEAttribute* instance is included, the parallel CMS signature, the external CMS signature or any data, e.g. a file or signatures other than CMS (JSON signature etc.). The semantics of the *ObjectRef* fields of the *dataObjectRefs* field are as follows:

— If the value of the *poEObjectRef.type* field does not define the type of data objects the *type* field of the *ObjectRef* fields of the optional *dataObjectRefs* field shall be used for identification of the type of data object. If a CMS signature is referenced, the *type* field contains *id-signedData* OID (see IETF RFC 5652, Section 5.1). If arbitrary octet strings are referenced, the *type* field contains *id-data* OID (see IETF RFC 5652, Section 4), such as ASCII or UTF-8 text files; the interpretation is left up to the application whether it will use the value of the *contentDescription* field containing, e.g. MIME *Content-Type*.

— The *objectId* field is either of the *DSId* type covering a digital signature of data object or of the *DId* type covering the whole data object.

— The optional *location* field shall be the URL location of the data object, as specified in Annex D. See IETF RFC 8089 or IETF RFC 7230, Section 2.7, where URI is used throughout HTTP as the means for identifying resources or Annex D for additional rules when the ASN.1 object is stored in a ZIP, PDF container or in another ASN.1 object. The optional *location* field shall be not included when the *type* field contains *id-signedData* OID and the data object is the object of the CMS signature (the *SignerInfo*

