ICS 35.240.63 SLOVENSKÁ TECHNICKÁ NORMA Máj 2021

STN	**Procesy, dátové prvky a dokumenty v obchode, priemysle a administratíve Dlhodobé profily podpisov Časť 4: Atribúty ukazujúce na (externé) dôkazy o existencii objektov používaných vo formátoch dlhodobého podpisu (PoE Atribúty)**	**STN ISO 14533-4** 97 4104

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

Táto norma obsahuje anglickú verziu ISO 14533-4: 2019.

This standard includes the English version of ISO 14533-4: 2019.

132548

Anotácia

Tento dokument poskytuje podrobné informácie spojené s analýzou, výberom a implementáciou postupov spojených s dlhodobými podpismi. Vypracovanie tohto dokumentu je výsledkom organizačných požiadaviek na získanie informácií o už existujúcich objektoch definovaných v technologických štandardoch, technických správach a osvedčených postupoch odvetvia pre elektronické podpisy, ktoré sú dlhodobo overiteľné. Účelom tohto dokumentu je zabezpečiť interoperabilitu implementácií, pokiaľ ide o dlhodobé podpisy, ktoré umožňujú dlhodobú overiteľnosť elektronických podpisov. Tento dokument objasňuje podmienky použité v procese validácie na zabezpečenie úplného a nezmeniteľného výsledku.

Národný predhovor

Normatívne referenčné dokumenty

Nasledujúce dokumenty, celé alebo ich časti, sú v tomto dokumente normatívnymi odkazmi a sú nevyhnutné pri jeho používaní. Pri datovaných odkazoch sa použije len citované vydanie. Pri nedatovaných odkazoch sa použije najnovšie vydanie citovaného dokumentu (vrátane všetkých zmien).

POZNÁMKA 1. – Ak bola medzinárodná publikácia zmenená spoločnými modifikáciami, čo je indikované označením (mod), použije sa príslušná EN/HD.

POZNÁMKA 2. – Aktuálne informácie o platných a zrušených STN možno získať na webovej stránke www.unms.sk.

ISO/IEC 8825-1 dosiaľ nezavedená

ISO/IEC 9594-8 dosiaľ nezavedená

ISO 32000-2 dosiaľ nezavedená

ETSI EN 319 122-1 V1.1.1: 2016 zavedená v STN EN 319 122-1 V1.1.1: 2017 Elektronické podpisy a infraštruktúry (ESI). Digitálne podpisy vo formáte CAdES. Časť 1: Stavebné bloky a základné podpisy vo formáte CadES (87 9122)

IETF RFC 3161 dosiaľ nezavedená

IETF RFC 6960 dosiaľ nezavedená

IETF RFC 4648 dosiaľ nezavedená

IETF RFC 4998 dosiaľ nezavedená

IETF RFC 6283 dosiaľ nezavedená

IETF RFC 5652 dosiaľ nezavedená

Vypracovanie normy

Spracovateľ: Úrad pre normalizáciu, metrológiu a skúšobníctvo SR, Bratislava

Technická komisia: TK 37 Informačné technológie

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)*

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.