

<b>STN</b>	<b>Procesy, dátové prvky a dokumenty v obchode, priemysle a administratíve Dlhodobé profily podpisov Časť 2: Profily dlhodobého podpisu zaručených elektronických podpisov vo formáte XML (XAdES)</b>	<b>STN ISO 14533-2</b>  97 4104
------------	---	---

Processes, data elements and documents in commerce, industry and administration  
Long term signature profiles  
Part 2: Long term signature profiles for XML Advanced Electronic Signatures (XAdES)

Processus, éléments d'informations et documents dans le commerce, l'industrie et l'administration  
Profils de signature à long terme  
Partie 2: Profils de signature à long terme pour les signatures électroniques avancées XML (XAdES)

Prozesse, Datenelemente und Dokumente in Handel, Industrie und Verwaltung  
Langzeitsignaturprofile  
Teil 2: Langzeitsignaturprofile für XML Advanced Electronic Signatures (XAdES)

Táto norma obsahuje anglickú verziu ISO 14533-2: 2012.

This standard includes the English version of ISO 14533-2: 2012.

**132937**

## **Anotácia**

Táto časť ISO 14533 špecifikuje prvky, ktoré sú definované v XML Advanced Electronic Signatures (XAdES) a ktoré umožňujú overenie digitálneho podpisu po dlhú dobu.

Neposkytuje nové technické špecifikácie týkajúce sa samotného digitálneho podpisu ani nové obmedzenia týkajúce sa použitia technických špecifikácií týkajúcich sa digitálnych podpisov, ktoré už existujú.

## **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](http://www.unms.sk).

ETSI/TS 101 903 v 1.4.1 (2009-06) dosiaľ nezavedená

### **Vypracovanie normy**

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

Technická komisia: TK 37 Informačné technológie

<b>Contents</b>	<b>Page</b>
<b>Foreword</b> .....	<b>iv</b>
<b>Introduction</b> .....	<b>v</b>
<b>1 Scope</b> .....	<b>1</b>
<b>2 Normative references</b> .....	<b>1</b>
<b>3 Terms and definitions</b> .....	<b>1</b>
<b>4 Symbols</b> .....	<b>2</b>
<b>5 Requirements</b> .....	<b>2</b>
<b>6 Long term signature profiles</b> .....	<b>2</b>
<b>6.1 Defined profiles</b> .....	<b>2</b>
<b>6.2 Representation of the required level</b> .....	<b>3</b>
<b>6.3 Standard for setting the required level</b> .....	<b>3</b>
<b>6.4 Action to take when an optional element is not implemented</b> .....	<b>4</b>
<b>6.5 XAdES-T profile</b> .....	<b>4</b>
<b>6.6 XAdES-A profile</b> .....	<b>6</b>
<b>6.7 Timestamp validation data</b> .....	<b>8</b>
<b>Annex A (normative) Supplier's declaration of conformity and its attachment</b> .....	<b>9</b>
<b>Annex B (normative) Structure of timestamp token</b> .....	<b>14</b>
<b>Bibliography</b> .....	<b>16</b>

**ISO 14533-2:2012(E)****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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

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.

ISO 14533-2 was prepared by Technical Committee ISO/TC 154, *Processes, data elements and documents in commerce, industry and administration*.

ISO 14533 consists of the following parts, under the general title *Processes, data elements and documents in commerce, industry and administration — Long term signature profiles*:

- *Part 1: Long term signature profiles for CMS Advanced Electronic Signatures (CAAdES)*
- *Part 2: Long term signature profiles for XML Advanced Electronic Signatures (XAdES)*

## Introduction

The purpose of this part of ISO 14533 is to ensure the interoperability of implementations with respect to long term signatures that make electronic signatures verifiable for a long term. Long term signature specifications referenced by each implementation cover XML Advanced Electronic Signatures (XAdES) developed by the European Telecommunications Standards Institute (ETSI).

# Processes, data elements and documents in commerce, industry and administration — Long term signature profiles —

## Part 2: Long term signature profiles for XML Advanced Electronic Signatures (XAdES)

### 1 Scope

This part of ISO 14533 specifies the elements, among those defined in XML Advanced Electronic Signatures (XAdES), that enable verification of a digital signature over a long period of time.

It does not give new technical specifications about the digital signature itself, nor new restrictions of usage of the technical specifications about the digital signatures which has already existed.

NOTE XML Advanced Electronic Signatures (XAdES) is the extended specification of XML-Signature Syntax and Processing, used widely.

### 2 Normative references

The following referenced documents are indispensable for the application 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 14533-1, *Processes, data elements and documents in commerce, industry and administration — Long term signature profiles – Part 1: Long term signature profiles for CMS Advanced Electronic Signatures (CAAdES)*

ETSI TS 101 903 v1.4.1 (2009-06), *XML Advanced Electronic Signatures (XAdES)* <sup>1)</sup>

**koniec náhľadu – text ďalej pokračuje v platenej verzii STN**

1) Available from <http://pda.etsi.org/pda/queryform.asp>.