ČESKÁ TECHNICKÁ NORMA

ICS 35.240.60 **Duben 2014**

Procesy, datové prvky a dokumenty v obchodě, průmyslu a státní správě – Profily dlouhodobého podpisu – Část 1: Profily dlouhodobého podpisu zaručených elektronických podpisů v standardu CMS (CAdES)

ČSN ISO 14533-1
36 9796

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 (CAdES)

Processus, éléments d,informations et documents dans le commerce, l,industrie et l,administration – Profils de signature
a long terme –
Partie 1: Profils de signature a long terme pour les signatures électroniques avancées CMS (CAdES)

Tato norma je českou verzí mezinárodní normy ISO 14533-1:2012. Překlad byl zajištěn Úřadem pro technickou normalizaci, metrologii a státní zkušebnictví. Má stejný status jako oficiální verze.

This standard is the Czech version of the International Standard ISO 14533-1:2012. It was translated by the Czech Office for Standards, Metrology and Testing. It has the same status as the official version.

Národní předmluva

Informace o citovaných dokumentech

ETSI TS 101 733 v1.8.1:2009 nezavedena

Souvisící ČSN

ČSN ISO/IEC 18014-2 (36 9795) Informační technologie – Bezpečnostní techniky – Služby pro vyznačení času –
Část 2: Mechanismy vytvářející nezávislé tokeny

Vypracování normy

Zpracovatel: Ing. Jindřich Kodl, CSc., IČ 63957108

Technická normalizační komise: TNK 20, Informační technologie

Pracovník Úřadu pro technickou normalizaci, metrologii a státní zkušebnictví: Ing. Miroslav Škop

MEZINÁRODNÍ NORMA

Procesy, datové prvky a dokumenty v obchodě, ISO 14533-1
průmyslu a státní správě – Profily dlouhodobého podpisu První vydání
Část 1: Profily dlouhodobého podpisu zaručených 2012-09-15
elektronických podpisů v standardu CMS (CAdES)

ICS 35.240.60

Obsah

Strana

ISO copyright office

Case postale 56 · CH-1211 Geneva 20

Tel. + 41 22 749 01 11

Fax + 41 22 749 09 47

E-mail copyright@iso.org

Web www.iso.org

Published in Switzerland

Předmluva

ISO (Mezinárodní organizace pro normalizaci) je celosvětová federace národních normalizačních orgánů (členů ISO). Mezinárodní normy obvykle vypracovávají technické komise ISO. Každý člen ISO, který se zajímá o předmět, pro který byla vytvořena technická komise, má právo být v této technické komisi zastoupen. Práce se zúčastňují také vládní i nevládní mezinárodní organizace, s nimiž ISO navázala pracovní styk. ISO úzce spolupracuje s Mezinárodní elektrotechnickou komisí (IEC) ve všech záležitostech normalizace v elektrotechnice.

Návrhy mezinárodních norem jsou vypracovávány v souladu s pravidly danými směrnicemi ISO/IEC, část 2.

Hlavním úkolem technických komisí je vypracování mezinárodních norem. Návrhy mezinárodních norem přijaté technickými komisemi se rozesílají členům ISO k hlasování. Vydání mezinárodní normy vyžaduje souhlas alespoň 75 % hlasujících členů.

Upozorňuje se na možnost, že některé prvky tohoto dokumentu mohou být předmětem patentových práv. ISO nelze činit odpovědnou za identifikaci jakéhokoliv nebo všech patentových práv.

ISO 14533-1 vypracovala technická komise ISO/TC 154 *Procesy, datové prvky a dokumenty v obchodě*.

ISO 14533 se skládá z následujících částí se společným názvem *Procesy, datové prvky a dokumenty v obchodě, průmyslu a státní správě – Profily dlouhodobého podpisu*:

- *Část 1: Profily dlouhodobého podpisu zaručených elektronických podpisů v standardu CMS (CAdES*
- *Část 2: Profily dlouhodobého podpisu zaručených elektronických podpisů v standardu XML (XAdES)*

1 Předmět normy

Tato část ISO 14533 specifikuje prvky, definované v CMS pro zaručené elektronické podpisy (CAdES), které umožňují ověřitelnost digitálního podpisu na dlouhé časové období.

Neposkytuje nové technické specifikace o digitálních podpisech jako takových, ani nová omezení použití technických specifikací, týkajících se digitálních podpisů, které již existují.

POZNÁMKA Zaručené elektronické podpisy dle CMS (CAdES) jsou rozšířenou specifikací široce používané syntaxe kryptografických zpráv (CMS).