ČESKÁ TECHNICKÁ NORMA

ICS 35.040 **Srpen 2013**

Informační technologie – Bezpečnostní techniky – Služby pro vyznačení času – Část 1: Struktura

ČSN ISO/IEC 18014-1
36 9795

Information technology – Security techniques – Time-stamping services – Part 1: Framework

Technologies de l,information – Techniques de sécurité – Services d,estampillage de temps – Partie 1: Cadre général

Tato norma je českou verzí mezinárodní normy ISO/IEC 18014-1:2008. 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/IEC 18014-1:2008. 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

ISO 8601 zavedena v ČSN ISO 8601 (97 9738) Datové prvky a formáty výměny – Výměna informací – Zobrazení data a času

ISO/IEC 10118 (všechny části) (36 9930) Informační technologie – Bezpečnostní techniky – Hašovací funkce

Souvisící ČSN

ČSN ISO/IEC TR 14516:2004 (36 9791) Informační technologie – Bezpečnostní techniky – Směrnice pro používání a řízení služeb důvěryhodných třetích stran

ČSN ISO/IEC 8824-1:2010 (36 9632) Informační technologie – Abstraktní syntaxe způsobu zápisu jedna (ASN.1): Specifikace základního způsobu zápisu

ČSN ISO/IEC 8824-2:2013 (36 9632) Informační technologie – Abstraktní syntaxe způsobu zápisu jedna (ASN.1): Specifikace informačního objektu

ČSN ISO/IEC 9798-1:2011 (36 9743) Informační technologie – Bezpečnostní techniky – Autentizace entit –

Část 1: Všeobecně

ČSN ISO 19108:2003 (97 9827) Geografická informace – Časové schéma

Vysvětlivky k textu převzaté normy

1) Anglický termín „Time-stamping“ je pro účely této normy překládán jako „vyznačení času“.

2) Anglický termín „nonce“ je ponechán bez překladu.

3) Anglický termín „Message digest“ je pro účely této normy překládán jako „otisk zprávy“.

4) Anglický termín „symbol“ se překládá českým slovem symbol, protože se zde používá ve významu nadřazeného termínu vůči podřazeným termínům: značky, znaky, označení atd., aby se všechny tyto termíny nemusely vypisovat.

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

Informační technologie – Bezpečnostní techniky – ISO/IEC 18014-1
Služby pro vyznačení času – Druhé vydání
Část 1: Struktura 2008-09

ICS 35.040

Obsah

Odmítnutí odpovědnosti za manipulaci s PDF souborem
Tento soubor PDF může obsahovat vložené typy písma. V souladu s licenční politikou Adobe lze tento soubor tisknout nebo prohlížet, ale nesmí být editován, pokud nejsou typy písma, které jsou vloženy, používány na základě licence a instalovány v počítači, na němž se editace provádí. Při stažení tohoto souboru přejímají jeho uživatelé odpovědnost za to, že nebude porušena licenční politika Adobe. Ústřední sekretariát ISO nepřejímá za její porušení žádnou odpovědnost.
Adobe je obchodní značka „Adobe Systems Incorporated".
Podrobnosti o softwarových produktech použitých k vytvoření tohoto souboru PDF lze najít ve Všeobecných informacích, které se vztahují k souboru; parametry, na jejichž základě byl PDF soubor vytvořen, byly optimalizovány pro tisk. Soubor byl zpracován s maximální péčí tak, aby ho členské organizace ISO mohly používat. V málo pravděpodobném případě, že vznikne problém, který se týká souboru,
informujte o tom Ústřední sekretariát ISO na níže uvedené adrese.

DOKUMENT CHRÁNĚNÝ COPYRIGHTEM

© ISO/IEC 2008

Veškerá práva vyhrazena. Pokud není specifikováno jinak, nesmí být žádná část této publikace reprodukována nebo používána v jakékoliv formě nebo jakýmkoliv způsobem, elektronickým nebo mechanickým, včetně fotokopií a mikrofilmů, bez písemného svolení buď od organizace ISO na níže uvedené adrese, nebo od členské organizace ISO v zemi žadatele.

ISO/IEC 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) a IEC (Mezinárodní elektrotechnická komise) tvoří specializovaný systém celosvětové normalizace. Národní orgány, které jsou členy ISO nebo IEC, se podílejí na vypracování mezinárodních norem prostřednictvím technických komisí ustavených příslušnými organizacemi pro jednotlivé obory technické činnosti. Technické komise ISO a IEC spolupracují v oborech společného zájmu. Práce se zúčastňují také další vládní a nevládní mezinárodní organizace, s nimiž ISO a IEC také navázaly pracovní styk. V oblasti informační technologie zřídily ISO a IEC společnou technickou komisi ISO/IEC JTC 1.

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

Hlavním úkolem společné technické komise je vypracování mezinárodních norem. Návrhy

mezinárodních norem přijaté společnou technickou komisí jsou rozesílány národním členům k hlasování. Vydání mezinárodní normy vyžaduje souhlas alespoň 75 % hlasujících národních orgánů.

Upozorňuje se na možnost, že některé prvky tohoto dokumentu mohou být předmětem patentových práv. ISO a IEC nelze činit odpovědnými za identifikování jakéhokoliv nebo všech patentových práv.

ISO/IEC 18014-1 vypracovala společná technická komise ISO/IEC JTC 1, *Informační technologie,* subkomise SC 27, IT *Bezpečnostní techniky.*

Toto druhé vydání zrušuje a nahrazuje první vydání (ISO/IEC 18014-1:2002), jehož je technickou revizí.

ISO/IEC 18014 se skládá z následujících částí se společným názvem „*Informační technologie – Bezpečnostní techniky – Služby pro vyznačení času*“

- *Část 1: Struktura*
- *Část 2: Mechanismy vytvářející nezávislé tokeny*
- *Část 3: Mechanismy vytvářející propojené tokeny*

Úvod

Mezinárodní organizace pro normalizaci (ISO) a (Mezinárodní elektrotechnická komise (IEC) upozorňují na to, že je třeba věnovat pozornost skutečnosti, že shoda s touto mezinárodní normou může zahrnovat použití patentů.

ISO a IEC nezaujímají stanovisko k evidenci, platnosti a rozsahu tohoto patentového práva.

Držitelé tohoto patentového práva ujistili ISO a IEC, že jsou ochotni s uživateli na celém světě dohodnout licence za přiměřených a nediskriminačních podmínek. V tomto ohledu jsou prohlášení držitelů těchto patentových práv registrována u ISO a IEC. Informace lze získat u:

ISO/IEC JTC 1/SC 27 Standing Document 8 (SD 8) „*Patent Information*“

SD 8 je veřejně dostupný na: http://www.din.de/ni/sc27

Upozorňuje se na možnost, že některé prvky této mezinárodní normy mohou být předmětem jiných patentových práv než takových, které byly uvedeny výše. ISO a IEC nelze činit odpovědnými za identifikování jakéhokoliv nebo všech patentových práv.

1 Předmět normy

Tato část ISO/IEC 18014:

- identifikuje cíl autority pro vyznačení času;
- popisuje všeobecný model, na kterém jsou založeny služby pro vyznačení času;
- definuje služby pro vyznačení času;
- definuje základní protokoly mezi zúčastněnými entitami.

Konec náhledu - text dále pokračuje v placené verzi ČSN.