

**Informační technologie - Bezpečnostní techniky -
Služby pro vyznačení času -
Část 2: Mechanismy vytvářející nezávislé tokeny**

ČSN
ISO/IEC 18014-2
36 9795

Information technology - Security techniques - Time-stamping services -
Part 2: Mechanisms producing independent tokens

Technologies de l'information - Techniques de sécurité - Services d'estampillage de temps -
Partie 2: Mécanismes produisant des jetons indépendants

Tato norma je českou verzí mezinárodní normy ISO/IEC 18014-2:2009. 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 18014-2:2009. 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/IEC 8824-1:1998 nezavedena

ISO/IEC 9594-8:2005 dosud nezavedena

ISO/IEC 18014-1:2008 zavedena v ČSN ISO/IEC 18014-1:2013 (36 9795) Informační technologie -
Bezpečnostní techniky - Služby pro vyznačení času - Část 1: Struktura

Související ČSN

ČSN ISO 7498-2:1993 (36 9615) Systémy na spracovanie informácií. Prepojenie otvorených systémov (OSI). Základný referenčný model. Část 2: Bezpečnostná architektúra

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

ČSN ISO/IEC 8824-3:2013 (36 9632) Informační technologie - Abstraktní syntaxe způsobu zápisu jedna (ASN.1): Specifikace informačního objektu

ČSN ISO/IEC 8824-4:2013 (36 9632) Informační technologie - Abstraktní syntaxe způsobu zápisu jedna (ASN.1): Specifikace informačního objektu

ČSN ISO/IEC 8825-1:2012 (36 9625) Informační technologie – Pravidla kódování pro ASN.1: Specifikace základních pravidel kódování (BER), kanonických pravidel kódování (CER) a rozlišujících pravidel kódování (DER)

ČSN ISO/IEC 9797-1:2013 (36 9782) Informační technologie – Bezpečnostní techniky – Kódy pro autentizaci zprávy (MACs) – Část 1: Mechanismy používající blokovou šifru

ČSN ISO/IEC 9797-2:2013 (36 9782) Informační technologie – Bezpečnostní techniky – Kódy pro autentizaci zprávy (MACs) – Část 2: Mechanismy používající dedikovanou hašovací funkci

ČSN ISO/IEC 9798 (všechny části) (36 9743) Informační technologie – Bezpečnostní techniky – Autentizace entit – Část 1: Všeobecně

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

ČSN ISO/IEC 10181-1:1998 (36 9694) Informační technologie – Propojení otevřených systémů – Bezpečnostní struktury otevřených systémů: Přehled

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

Vysvětlivky k textu převzaté normy

- 1) Anglický termín „Time-stamping“ je pro účely této normy překládán jako „vyznačení času“.
- 2) Anglický termín „link“ je podle významu překládán jako „propojení“, „spojení“ nebo „sestava“.
- 3) 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 18014-2

Služby pro vyznačení času – Druhé vydání

Část 2: Mechanismy vytvářející nezávislé tokeny 2009-12

ICS 35 040

Obsah

Předmluva 5

1 Předmět normy 6

2 Citované dokumenty 6

3 Termíny a definice 6

4 Značení, symboly a zkratky 9

5 Služby vyznačení času 9

6 Tokeny vyznačení času 10

6.1 Obsah 10

6.2 Značení 10

6.3 Ověření 11

6.4 Obnovení 11

6.5 Ověření obnovení 11

7 Mechanismy ochrany 12

8 Nezávislé tokeny vyznačení času 12

8.1 Hlavní struktura 12

8.2 Rozšíření 13

8.3 Mechanismy ochrany 13

8.3.1 Digitální podpisy používající SignedData 13

8.3.2 Kódy autentizace zprávy používající AuthenticatedData 14

8.3.3 Archivace 15

8.3.4 Digitální podpisy používající SignerInfo 15

8.3 Protokoly 17

Příloha A (normativní) ASN.1 Modul pro vyznačení času 18

Příloha B (informativní) Kryptografická syntexe 24

B.1 Podepsaná data 25

B.2 Autentizovaná data 26

B.3 Archivovaná data 27

B.4 SignerInfo 28

Bibliografie 30

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 nepřijímá 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 fotokopíí 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 směrnici 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 18014-2 vypracovala společná technická komise ISO/IEC JTC1, *Informační technologie*, subkomise SC 27, *Bezpečnostní techniky*.

Toto druhé vydání zrušuje a nahrazuje první vydání (ISO/IEC 18014-2:2002), 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*

1 Předmět normy

Tato část ISO/IEC 18014 představuje obecný rámec pro poskytování služeb vyznačení času.

Služby vyznačení času mohou vytvářet, obnovovat a ověřovat tokeny vyznačení času.

Tokeny vyznačení času jsou spojením mezi daty a časovými okamžiky a jsou vytvořeny tak, aby prokázaly, že údaje existovaly v příslušném datu a čase. Kromě toho mohou být použity službami neodmítnutelnosti činností.

Tato část ISO/IEC 18014 specifikuje mechanismy, které generují nezávislá vyznačení času, s cílem ověřit nezávislé tokeny vyznačení času, ověřovatelé nepotřebují mít přístup k jiným tokenům vyznačení času. To znamená, že tokeny vyznačení času nejsou propojeny, jako je tomu v případě tokenů definovaných v ISO/IEC 18014-3.

Konec náhledu - text dále pokračuje v placené verzi ČSN.