

**Informační technologie - Bezpečnostní techniky -
Služby pro vyznačení času -
Část 3: Mechanismy vytvářející propojené tokeny**

ČSN
ISO/IEC 18014-3
36 9795

Information technology - Security techniques - Time-stamping services -
Part 3: Mechanisms producing linked tokens

Technologies de l'information - Techniques de sécurité - Services d'estampillage de temps -
Partie 3: Mécanismes produisant des jetons liés

Tato norma je českou verzí mezinárodní normy ISO/IEC 18014-3:2009. 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 18014-3:2009. 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 10118 (všechny části) zavedeny v ČSN ISO/IEC 10118 (36 9930) Informační technologie - Bezpečnostní techniky - Hašovací funkce

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

Souvisící ČSN

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

Vysvětlivky k textu převzaté normy

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

4) Anglické termíny „instance“ a „item“ jsou podle významu překládány jako „položka“.

5) Anglický termín „digest“ je překládán jako „otisk“.

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 18014-3

Služby pro vyznačení času – Druhé vydání

Část 3: Mechanismy vytvářející propojené tokeny 2009-12

ICS 35.040

Obsah

Strana

Předmluva 6

Úvod 7

1 Předmět normy 8

2 Citované dokumenty 8

3 Termíny a definice 8

4 Obecná diskuse 9

5 Operace specifické pro TSA vytvářející propojené tokeny 10

5.1 Operace propojování 10

5.2 Operace agregace 10

5.3 Operace zveřejnění 11

5.4 Operace rozšíření 11

6 Formáty zprávy 11

6.1 Žádost o vyznačení času 11

6.2 Odpověď na vyznačení času 12

6.3	Žádost o ověření	12
6.4	Odpověď na ověření	12
6.5	Žádost o rozšíření	13
6.6	Odpověď na rozšíření	13
7	Typy dat	14
7.1	Identifikátory objektu	14
7.2	TSTInfo	14
7.3	Token vyznačení času	15
7.4	BindingInfo	15
7.5	Řetězec	16
7.6	Propojení	16
7.7	Uzel	17
7.8	PublicationInfo	17
7.9	Rozšíření	18
8	Generování tokenů vyznačení času	19
8.1	Obecně	19
8.2	Zapouzdření DigestedData	20
8.3	Zapouzdření SignedData	20
8.4	Posouzení bezpečnosti	21
9	Ověření tokenu vyznačení času	21
9.1	Obecně	21
9.2	Zapouzdření DigestedData	21
9.3	Zapouzdření SignedData	21
9.4	Posouzení bezpečnosti	22
10	Rozšíření tokenu vyznačení času	22
11	Obnovení tokenu vyznačení času	22
11.1	Obecně	22

11.2 Operace obnovení a ověření 23

11.3 Operace obnovení a rozšíření 23

Příloha A (normativní) ASN.1 Moduly vyznačení času 24

Příloha B (informativní) Další diskuse 29

Příloha C (informativní) Datová struktura 33

C.1 Tokeny vyznačení času používající zapouzdření DigestedData 33

C.2 Tokeny vyznačení času používající zapouzdření SignedData 34

C.3 Propojování lineárního řetězce s agregací Merkleho stromem 35

Bibliografie 37

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 2009

Veškerá práva vyhrazena. Pokud není specifikováno jinak, nesmí být žádná část této publikace reprodukována nebo používána v jakémkoliv 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 Genève 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 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 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 jakéhokoli nebo všech patentových práv.

ISO/IEC 18014-3 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 18014-3:2004), 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:

- popisuje obecný model služeb pro vyznačení času, vytvářející propojené tokeny;
- popisuje základní komponenty používané k vytvoření služby pro vyznačení času, vytvářející propojené tokeny;
- definuje datové struktury používané k interakci se službou pro vyznačení času, vytvářející propojené tokeny;
- popisuje specifické případy služeb pro vyznačení času, vytvářejících propojené tokeny;
- definuje protokol, který má být použit službami pro vyznačení času, vytvářejících propojené tokeny s cílem rozšíření propojených tokenů na uveřejněné hodnoty.

Konec náhledu - text dále pokračuje v placené verzi ČSN.