

2006

| | |
|------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------|
| 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'horodatage - Partie 3: Mécanismes produisant des jetons liés

Tato norma je českou verzí mezinárodní normy ISO/IEC 18014-3:2004. Mezinárodní norma ISO/IEC 18014-3:2004 má status české technické normy.

This standard is the Czech version of the International Standard ISO/IEC 18014-3:2004. The International Standard ISO/IEC 18014-3:2004 has the status of a Czech Standard.

| | |
|------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| The logo of the Czech Normalization Institute (ČNI) consists of the letters 'čni' in a stylized, lowercase font, followed by a solid grey rectangle. | © Český normalizační institut, 2006 76614 Podle zákona č. 22/1997 Sb. smějí být české technické normy rozmnožovány a rozšiřovány jen se souhlasem Českého normalizačního institutu. |
|------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

9671) Informační technologie - Propojení otevřených systémů - Adresář: Základní struktury certifikátu veřejného klíče a certifikátu atributu

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

ISO/IEC 18014-1:2002 zavedena v ČSN ISO/IEC 18014-1 (36 9795) Informační technologie - Bezpečnostní techniky - Služby pro vyznačení času - Část 1: Struktura

Vysvětlivky k textu převzaté normy

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

Vypracování normy

Zpracovatel: Ing. Alena Hönigová, IČ 61470716

Technická normalizační komise: TNK 42, Výměna dat

Pracovník Českého normalizačního institutu: Ing. Petr Wallenfels

Strana 3

MEZINÁRODNÍ NORMA

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

ISO/IEC 18014-3
První vydání
2004-02

Odmítavé stanovisko k 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, ledaže by typy písma, které jsou vloženy, byly 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 jsou k souboru připojeny; parametry, pomocí kterých 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, tj. když vznikne problém, který se týká souboru, informujte o tom na níže uvedené adrese Ústřední sekretariát ISO.

© ISO 1999

Všechna práva vyhrazena. ®ádná část této normy nesmí být reprodukována nebo zpracována

jakoukoliv jinou formou, jako například elektronickou, mechanickou, včetně fotokopíí a mikrofilmu bez písemného povolení ISO. Povolení lze vyžádat na níže uvedené adrese nebo u členské národní organizace v zemi žadatele.

ISO copyright office

Case postale 56, CH-1211 Geneva 20

Tel. +41 22 749 01 11

Fax. +41 22 734 10 79

e-mail copyright@iso.ch

Web www.iso.ch

Strana 4

Obsah

Strana

Úvod

.....
..... 6

1 Předmět
normy

.....
.. 7

2 Citované normativní
dokumenty.....

7

3 Termíny a
definice

..... 7

4 Všeobecná
diskuse

..... 8

5
Operace

.....
..... 8

5.1
Propojení

.....
..... 9

5.2

Agregace

..... 9

5.3

Zveřejnění

..... 9

6 Datové
struktury

..... 9

6.1 Identifikátory
objektů

..... 9

6.2

Uzel

..... 9

6.3

Propojení

..... 10

6.4

Řetězec

..... 10

6.5

BindingInfo

..... 11

6.6

Rozšíření

..... 11

6.6.1 Rozšíření žádosti a
tokenu..... 12

6.6.2 Rozšíření
BindingInfo

..... 13

7 Žádost o vyznačení
času..... 13

| | | |
|------------------|--------------------------------------------------|----|
| 8 | Odezva na vyznačení času..... | 14 |
| 8.1 | Zhuštění DigestedData | 15 |
| 8.2 | Zhuštění SignedData | 15 |
| 9 | Ověření vyznačení času..... | 16 |
| Příloha A | (normativní) ASN.1 Modul pro vyznačení času..... | 18 |
| Příloha B | (normativní) Další diskuse..... | 25 |
| Příloha C | (informativní) Datové struktury..... | 29 |
| | Bibliografie | 32 |

Předmluva

ISO (Mezinárodní organizace pro normalizaci) a IEC (mezinárodní elektrotechnická komise) tvoří specializovaný systém světové normalizace. Národní orgány, které jsou členy ISO a IEC, se podílejí na vývoji mezinárodních norem prostřednictvím technických komisí, zřízených příslušnou organizací a zabývajících se určitou oblastí technické činnosti. Technické komise ISO a IEC spolupracují v oblastech společných zájmů. Práce se zúčastňují i další mezinárodní organizace, vládní i nevládní, s nimiž ISO a IEC navázalo pracovní styk. ISO a IEC ustavily v oblasti informační technologie společnou technickou komisi, ISO/IEC JTC1.

Mezinárodní normy jsou navrhovány v souladu s pravidly obsaženými v části 2 Směrnic ISO/IEC.

Hlavním úkolem společné technické komise je příprava mezinárodních norem. Návrhy mezinárodních norem přijaté technickými komisemi se rozesílají národním orgánům k hlasování. Vydání mezinárodní normy vyžaduje souhlas alespoň 75 % z hlasujících členů.

Je třeba upozornit na to, že některé prvky tohoto dokumentu mohou být předmětem patentových práv. ISO a IEC nepřejímá odpovědnost za identifikaci některých nebo všech patentových práv.

ISO/IEC 18014-3 byla připravena společnou technickou komisí ISO/IEC JTC1, *Informační technologie*, subkomise SC 27, *Bezpečnostní techniky IT*.

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*

Mohou následovat další části.

Strana 6

Úvod

Mezinárodní organizace pro normalizaci (ISO) a Mezinárodní elektrotechnická komise (IEC) upozorňuje na to, že je třeba věnovat pozornost skutečnosti, že vyhovění této mezinárodní normě může zahrnovat použití patentů.

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

Držitel tohoto patentového práva ujistil ISO a IEC, že je ochoten dohodnout s uživateli na celém světě licence za rozumných a nediskriminačních okolností a podmínek. V tomto ohledu je prohlášení držitele tohoto patentovaného práva registrováno u ISO a IEC. Informace lze získat u:

ISO/IEC JTC 1/SC 27 Standing Dokument 8 (SD 8) "Patent Information"

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

Je třeba upozornit na to, že některé prvky této mezinárodní normy mohou být předmětem jiných patentových práv než těch, které jsou uvedeny výše. ISO a IEC nepřejímají odpovědnost za identifikaci některých nebo všech patentových práv.

Strana 7

1 Předmět normy

Tato část ISO/IEC 18014

- popisuje všeobecný model služeb pro vyznačení času vytvářejících propojené tokeny;
- popisuje základní komponenty používané ke konstrukci služby pro vyznačení času tohoto typu;
- definuje datové struktury používané k interakci se službami pro vyznačení času tohoto typu;
- popisuje specifické instance takovýchto služeb pro vyznačení času.

-- Vynechaný text --