

**2006**

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'horodatage - Partie 2:  
Mécanismes produisant  
des jetons indépendants

Informationstechnik - IT-Sicherheitsverfahren - Zeitstempeldienste - Teil 2: Zeitstempelmechanismen mit dedizierten  
Zeitstempeln

Tato norma je českou verzí mezinárodní normy ISO/IEC 18014-2:2002. Překlad byl zajištěn Českým normalizačním institutem. Má stejný status jako oficiální verze.

This standard is the Czech version of the International Standard ISO/IEC 18014-2:2002. It was translated by Czech Standards Institute. It has the same status as the official version.

The logo of the Czech Standards Institute (ČNI) consists of the lowercase letters 'cni' in a stylized, bold font, followed by a solid grey rectangle.	© Český normalizační institut, 2006 <b>76125</b> Podle zákona č. 22/1997 Sb. smějí být české technické normy rozmnožovány a rozšiřovány jen se souhlasem Českého normalizačního institutu.
---	--

## Národní předmluva

### Informace o citovaných normativních dokumentech

ISO 7498-2:1989 zavedena v ČSN ISO 7498-2: (1989) (36 9615) Systémy zpracování informací - Propojení otevřených systémů -Základní referenční model - Část 2: Bezpečnostní architektura

ISO/IEC 8824-1:1998 ITU-T Doporučení X.680 (1997) zavedena v ČSN ISO/IEC 8824-1:1998 (36 9632) Informační technologie - Abstraktní syntaktická notace jedna (ASN.1): Specifikace základní notace

ISO/IEC 8824-2:1998 ITU-T Doporučení X.681 (1997) zavedena v ČSN ISO/IEC 8824-2:1998 (36 9632) Informační technologie - Abstraktní syntaktická notace jedna (ASN.1): Specifikace informačních objektů

ISO/IEC 8824-3:1998 ITU-T Doporučení X.682 (1997) zavedena v ČSN ISO/IEC 8824-3:1998 (36 9632) Informační technologie - Abstraktní syntaktická notace jedna (ASN.1): Specifikace omezení

ISO/IEC 8824-4:1998 ITU-T Doporučení X.683 (1997) zavedena v ČSN ISO/IEC 8824-4:1998 (36 9632) Informační technologie - Abstraktní syntaktická notace jedna (ASN.1): Parametrizace specifikací ASN.1

ISO/IEC 8825-1:1998 ITU-T Doporučení X.690 (1997) zavedena v ČSN ISO/IEC 8825-1:1998 (36 9635) Informační technologie - Kódovací pravidla pro ASN.1: Specifikace základních kódovacích pravidel (BER), kanonických kódovacích pravidel (CER) a zvláštních kódovacích pravidel (DER)

ISO/IEC 9594-8:2001 ITU-T Doporučení X.509 (2000) zavedena v ČSN ISO/IEC 9594-8:2003 (36 9671) Informační technologie - Propojení otevřených systémů - Adresář: Základní struktury certifikátu veřejného klíče a certifikátu atributu

ISO/IEC TR 14516:2002 zavedena v ČSN ISO/IEC TR14516:2004 (36 9791), Informační technologie - Směrnice pro použití a řízení služeb důvěryhodných třetích stran

ISO/IEC 9798-1:1997 zavedena v ČSN ISO/IEC 9798-1 (36 9743) Informační technologie - Bezpečnostní techniky - Autentizace entit - Část 1: Všeobecně

ISO/IEC 10181-2:1996 zavedena v ČSN ISO/IEC 10181-2 (36 9694) Informační technologie - Bezpečnostní techniky - Struktura bezpečnosti pro otevřené systémy: Struktura autentizace

ISO/IEC 11770-1:1996 zavedena v ČSN ISO/IEC 11770-1 (36 9785) Informační technologie - Propojení otevřených systémů - Správa klíčů - Část 1: Struktura

ISO/IEC 11770-3:1997 zavedena v ČSN ISO/IEC 11770-3 (36 9785) Informační technologie - Bezpečnostní techniky - Správa klíčů - Část 3: Mechanismy používající asymetrické techniky

ISO/IEC 13888-1:1999 zavedena v ČSN ISO/IEC 14888-2 (36 9788) Informační technologie - Bezpečnostní techniky - Nepopiratelnost - Část 1: Všeobecně

ISO/IEC 14888 (všechny části) zavedena v ČSN ISO/IEC 14888 (36 9788) Informační technologie - Bezpečnostní techniky - Digitální podpisy s dodatkem

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 20, Informační technologie

Pracovník Českého normalizačního institutu: Ing. Petr Wallenfels

Strana 3

MEZINÁRODNÍ NORMA	
Informační technologie - Bezpečnostní techniky - Služby pro vyznačení času - Část 2: Mechanismy vytvářející nezávislé tokeny	ISO/IEC 18014-2 První vydání 2002-12

**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 nepřijímá za její porušení žádnou odpovědnost.

Adobe je obchodní značka „Adobe Systems Incorporated“.

Podrobnosti o softwarových produktech použitých k vytváření 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. Žádná 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](mailto:copyright@iso.ch)

Web [www.iso.ch](http://www.iso.ch)

Obsah

Strana

Úvod

..... 6

**1**      Předmět  
normy

..... 6

**2**      Normativní  
odkazy

..... 6

**3**      Termíny a  
definice

..... 7

**4**      Všeobecná  
diskuse

..... 8

**5**      Entity procesu vyznačování  
času.....

9

**6**      Formáty  
zpráv

..... 9

**6.1**    Identifikátory  
objektů

..... 10

**6.2**    Pole  
rozšíření

..... 11

**6.2.1**    Rozšíření  
ExtHash

.....

.....	11
<b>6.2.2</b> Rozšíření ExtMethod	.....
.....	11
<b>6.2.3</b> Rozšíření ExtRenewal	.....
.....	11
<b>7</b> Vyznačení času používající digitální podpisy.....	11
<b>7.1</b> Odezva TSA	.....
.....	12
<b>7.2</b> Ověření tokenu	.....
.....	13
<b>8</b> Vyznačení času používající kódy pro autentizaci zprávy.....	13
<b>8.1</b> Odezva TSA	.....
.....	14
<b>8.2</b> Generování MAC	.....
.....	14
<b>8.3</b> Ověření MAC	.....
.....	15
<b>8.4</b> Ověření tokenu	.....
.....	15
<b>9</b> Vyznačení času používající archivování.....	15
<b>9.1</b> Odezva	

TSA	15
<b>9.2</b> Ověření tokenu	16
<b>Příloha A</b> (normativní) ASN.1 Modul pro vyznačení času	17
<b>Příloha B</b> (informativní) Datové struktury	23
Bibliografie	26

Strana 5

---

## 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.

ISO/IEC 18014-2 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.

## 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 Document 8 (SD 8) "Patent Information"*

SD 8 je veřejně dostupný na: <http://www.din.de/ni/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 nepřijímají odpovědnost za identifikaci některých nebo všech patentových práv.

## 1 Předmět normy

Služba pro vyznačení času poskytuje důkaz o tom, že datová položka existovala před určitým časovým okamžikem. Služby pro vyznačení času vytvářejí tokeny vyznačení času, což jsou datové struktury obsahující ověřitelné kryptografické svázání reprezentace datových položek a časové hodnoty. Tato část ISO/IEC 18014 stanovuje mechanismy vyznačení času vytvářející nezávislé tokeny, které mohou být ověřeny jeden po druhém.

---

**-- Vynechaný text --**