

2005

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

Informationstechnik - IT-Sicherheitsverfahren - Zeitstempeldienste - Teil 1: Rahmenangaben

Tato norma je českou verzí mezinárodní normy ISO/IEC 18014-1:2002. Mezinárodní norma ISO/IEC 18014-1:2002 má status české technické normy.

This standard is the Czech version of the International Standard ISO/IEC 18014-1:2002. The International Standard ISO/IEC 18014-1:2002 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, 2005 71864 Podle zákona č. 22/1997 Sb. smějí být české technické normy rozmnožovány a rozšiřovány jen se souhlasem Českého normalizačního institutu.
--	--

Citované normy

ISO 8601:2000 dosud nezavedena

ISO/IEC 8824-1:1998 i X.680:ITU-T Doporučení X.680 (1997) zavedena v ČSN ISO/IEC 8824-1:1998 i X.680:ITU-T Doporučení X.680 (1998) (36 9632) Informační technologie - Abstraktní syntaktická notace jedna (ASN.1): Specifikace základní notace, nahrazena ISO/IEC 8824-1:2002

ISO/IEC 8824-2:1998 i X.681:ITU-T Doporučení X.681 (1997) zavedena v ČSN ISO/IEC 8824-2:1998 i X.681 ITU-T Doporučení X.681 (1998) (36 9632) Informační technologie - Abstraktní syntaktická notace jedna (ASN.1): Specifikace informačních objektů, nahrazena ISO/IEC 8824-2:2002

ISO/IEC 8824-3:1998 i X.682:ITU-T Doporučení X.682 (1997) zavedena v ČSN ISO/IEC 8824-3:1998 i X.682 ITU-T Doporučení X.682 (1998) (36 9632) Informační technologie - Abstraktní syntaktická notace jedna (ASN.1): Specifikace omezení, nahrazena ISO/IEC 8824-3:2002

ISO/IEC 8824-4:1998 i X.683:ITU-T Doporučení X.683 (1997) zavedena v ČSN ISO/IEC 8824-4:1998 i X.683 ITU-T Doporučení X.683 (1998) (36 9632) Informační technologie - Abstraktní syntaktická notace jedna (ASN.1): Parametrizace specifikací ASN.1, nahrazena ISO/IEC 8824-4:2002

ISO/IEC 8825-1:1998iX.690:ITU-T Doporučení X.690 (1997) zavedena v ČSN ISO/IEC 8825-1:1998iX.690:ITU-T Doporučení X.690 (1998) (36 9635) Informační technologie - Kódovací pravidla pro ASN.1: Specifikace základních kódovacích pravidel (BER), kanonických kódovacích pravidel (CER) a zvláštních kódovacích pravidel (DER), nahrazena ISO/IEC 8825-1:2002

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

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

ISO/IEC 11770-3:1999 zavedena v ČSN ISO/IEC 11770-3 (36 9785) Informační technologie - Bezpečnostní techniky - Správa klíčů - Část 3: Mechanismy používající asymetrické techniky

ISO/IEC 14888-2:1999 zavedena v ČSN ISO/IEC 14888-2 (36 9788) Informační technologie - Bezpečnostní techniky - Digitální podpisy s dodatkem - Část 2: Mechanismy založené na identitě

ISO/IEC 14888-3:1999 zavedena v ČSN ISO/IEC 14888-3 (36 9788) Informační technologie - Bezpečnostní techniky - Digitální podpisy s dodatkem - Část 3: Mechanismy založené na certifikátu

ISO/IEC 15946-2:2002 dosud nezavedena

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 „výťah ze zprávy“.

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 1: Struktura

ISO/IEC 18014-1
První vydání
2002-10

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.

Všechna práva vyhrazena. Není-li uvedeno jinak, nesmí být žádná část této publikace reprodukována nebo zpracována jakoukoli jinou formou, jako jsou například elektronické nebo mechanické prostředky, včetně fotokopii a mikrofilmů, 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 22 749 09 47

E-mail copyright@iso.ch

Web www.iso.ch

Strana 4

Úvod	6
1 Předmět normy	7
2 Normativní odkazy	7
3 Termíny a definice	8
4 Všeobecná diskuse o vyznačení času	9
4.1 Entity v procesu vyznačení času	9
4.2 Vyznačení času	10
4.3 Používání vyznačení času	10
4.4 Ověření tokenů vyznačení času	11
4.5 Služby zahrnuté ve vyznačení času	11
5 Komunikace mezi zúčastněnými entitami	11
5.1 Transakce žádosti o vyznačení času	11
5.2 Transakce ověření vyznačení času	12
6 Formáty zpráv	

... 12

6.1 Žádost o vyznačení
času..... 12

6.2 Odezva na žádost o vyznačení
času..... 13

6.3 Ověření vyznačení
času..... 14

6.4 Pole
rozšíření
.....

... 15

Příloha A (normativní) ASN.1 Modul pro vyznačování
času..... 16

Příloha B (normativní) Výňatek ze syntaxe kryptografické
zprávy..... 21

Bibliografie
.....
..... 28

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 3 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 této části ISO/IEC 18014 mohou být předmětem patentových práv. ISO a IEC nepřijímá odpovědnost za identifikaci některých nebo všech patentových práv.

ISO/IEC 18014-1 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.

Přílohy A a B této části mezinárodní normy ISO/IEC 18014 jsou její nedílnou součástí.

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 části ISO/IEC 9796 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 části ISO/IEC 9796 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:

- 1 identifikuje úlohu autority pro vyznačení času;
- 2 popisuje všeobecný model, na kterém jsou služby pro vyznačení času založeny;
- 3 definuje služby pro vyznačení času;
- 4 definuje základní protokoly vyznačení času;

5 specifikuje protokoly mezi zúčastněnými entitami.

-- Vynechaný text --