ČESKÁ TECHNICKÁ NORMA

ICS 35.040

Únor 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.

Národní předmluva

Citované normy

ISO 8601:2000 dosud nezavedena

ISO/IEC 8824-1:1998 ï X.680:ITU-T Doporučení X.680 (1997) zavedena v ČSN ISO/IEC 8824-1:1998 ï 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 ï X.681:ITU-T Doporučení X.681 (1997) zavedena v ČSN ISO/IEC 8824-2:1998 ï 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 ï X.682:ITU-T Doporučení X.682 (1997) zavedena v ČSN ISO/IEC 8824-3:1998 ï 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 ï X.683:ITU-T Doporučení X.683 (1997) zavedena v ČSN ISO/IEC 8824-4:1998 ï 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 8825-1:1998ïX.690:ITU-T Doporučení X.690 (1997) zavedena v ČSN ISO/IEC 8825-1:1998ïX.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 „výtah ze zprávy“.

Vypracování normy

Zpracovatel: Ing. Alena Hönigová, IČ 61470716

Technická normalizační komise: TNK 42, Výměna dat

Pracovník Českého normalizačního institutu: Ing. Petr Wallenfels

MEZINÁRODNÍ NORMA
Informační technologie - Bezpečnostní techniky - Služby pro vyznačení času - Část 1: Struktura

ISO/IEC 18014-1
První vydání
2002-10

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

Obsah

Strana

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 nepřejímá 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.

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.

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 --