ČESKÁ TECHNICKÁ NORMA

ICS 35.040

Září

2006

Bezpečnostní techniky IT - Nepopiratelnost - Část 1: Všeobecně	ČSN ISO/IEC 13888-1 36 9787

IT Security techniques - Non-repudiation - Part 1: General

Techniques de sécurité dans les TI - Non-répudiation - Partie 1: Généralités

Tato norma je českou verzí mezinárodní normy ISO/IEC 13888-1:2004. Překlad byl zajištěn Českým normalizačním institutem. Má stejný status jako oficiální verze.

This standard is the Czech version of the International Standard ISO/IEC 13888-1:2004. It was translated by Czech Standards Institute. It has the same status as the official version.

Nahrazení předchozích norem

Touto normou se nahrazuje ČSN ISO/IEC 13888-1 (36 9787) z května 2001.

Národní předmluva

Informace o citovaných normativních dokumentech

ISO 7498-2:1989 zavedena v ČSN ISO 7498-2:1993 (36 9615) Systémy na spracovanie informácií - Prepojenie otvorených systémov (OSI) - Základný referenčný model - Čas» 2: Bezpečnostná architektúra

ISO/IEC 9594-8:1995 zavedena v ČSN ISO/IEC 9594-8:1999 (36 9671) Informační technologie - Propojení otevřených systémů - Adresář: Struktura autentizace

ISO/IEC 9796 (všechny části) zavedeny v ČSN ISO 9796 (36 9780) Informační technologie - Bezpečnostní techniky - Schéma digitálních podpisů poskytujících obnovu zprávy

ISO/IEC 9797 (všechny části) zavedeny v ČSN ISO/IEC 9797 (36 9782) Informační technologie - Bezpečnostní techniky - Kódy pro autentizaci zprávy (MAC)

ISO/IEC 9798-1:1997 dosud nezavedena

ISO/IEC 10118 (všechny části) zavedeny v ČSN ISO/IEC 10118-1 (36 9930) Informační technologie - Bezpečnostní techniky - Hašovací funkce

ISO/IEC 10181-1:1996 zavedena v ČSN ISO/IEC 10181-1:1998 (36 9694) Informační technologie - Propojení otevřených systémů - Bezpečnostní struktury otevřených systémů - Část 1: Přehled

ISO/IEC 10181-4:1997 zavedena v ČSN ISO/IEC 10181-4:1999 (36 9694) Informační technologie - Propojení otevřených systémů - Bezpečnostní struktury otevřených systémů - Část 4: Struktura nepopiratelnosti

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

ISO/IEC 13888-2:1998 zavedena v ČSN ISO/IEC 13888-2:2001 (36 9787) Informační technologie - Bezpečnostní techniky - Nepopiratelnost - Část 2: Mechanismy používající symetrické šifry

ISO/IEC 13888-3:1997 zavedena v ČSN ISO/IEC 13888-2:2001 (36 9787) Informační technologie - Bezpečnostní techniky - Nepopiratelnost - Část 3: Mechanismy používající asymetrické šifry

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

ISO/IEC 18014 (všechny části) zavedena v ČSN ISO/IEC 18014 (36 9795) (všechny části) Informační technologie - Bezpečnostní techniky - Služby pro vyznačení času

Vypracování normy

Zpracovatel: Ing. Vladimír Pračke, IČ 40654419

Technická normalizační komise: TNK 42 Výměna dat

Pracovník Českého normalizačního institutu: Ing. Petr Wallenfels

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

Prázdná strana

MEZINÁRODNÍ NORMA

Bezpečnostní techniky IT - Nepopiratelnost
ISO/IEC 13888-1
Část 1: Všeobecně

Druhé vydání

2004-06

ICS 35.040

Obsah

Strana

Předmluva

ISO (Mezinárodní organizace pro normalizaci) a IEC (Mezinárodní elektrotechnická komise) tvoří specializovaný systém světové normalizace. Národní orgány, které jsou členy ISO nebo IEC, se podílejí na vývoji mezinárodních norem prostřednictvím technických komisí, zřízených dotyčnou 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 navázaly pracovní styk. ISO a IEC ustavily v oblasti informačních technologií společnou technickou

komisi, ISO/IEC JTC 1.

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 společnou technickou komisí, se rozesílají národním orgánům k hlasování. Vydání návrhu jako mezinárodní normy vyžaduje souhlas alespoň 75 % hlasujících členů.

Pozornost je nutno věnovat možnosti, že některé prvky tohoto dokumentu mohou být předmětem patentových práv. ISO a IEC nelze považovat za odpovědné za identifikování některých nebo všech takových patentových práv.

ISO/IEC 13888-1:2004 byla připravena společnou technickou komisí ISO/IEC JTC 1, *Informační technologie,* subkomise SC 27, *Bezpečnostní techniky IT*.

Druhé vydání ruší a nahrazuje první vydání (ISO/IEC 13888-1:1997), které prošlo technickou revizí.

ISO/IEC 13888 se skládá z následujících částí se společným názvem *Bezpečnostní techniky IT - Nepopiratelnost*:

- *Část 1: Všeobecně*
- *Část 2: Mechanismy používající symetrické techniky*
- *Část 3: Mechanismy používající asymetrické techniky*

Úvod

Cílem služby nepopiratelnosti je vytvářet, shromažďovat, udržovat, zajistit dostupnost a ověřovat důkazy týkající se údajné události nebo činnosti, aby bylo možné řešit spory o tom, zda se událost nebo činnost vyskytla či nikoliv. Tato část ISO/IEC 13888 popisuje model mechanismů nepopiratelnosti poskytujících důkazy, které jsou založeny na kryptografických kontrolních hodnotách, vytvářených pomocí symetrických nebo asymetrických kryptografických technik. Mechanismy nepopiratelnosti, obecně použitelné pro různé služby nepopiratelnosti, jsou nejprve popsány a potom aplikovány na vybrané služby nepopiratelnosti jako:

– nepopiratelnost původu,

– nepopiratelnost doručení,

– nepopiratelnost podání,

– nepopiratelnost přenosu.

Služby nepopiratelnosti zajiš»ují důkaz: důkaz zajiš»uje (jednoznačnou) odpovědnost ve vztahu k jednotlivé události nebo činnosti. Entita odpovědná za danou činnost nebo spojená s danou událostí, vzhledem k níž je generován důkaz, je označována jako subjekt důkazu. Existují dva hlavní typy důkazů, jejichž povaha závisí na použitých kryptografických technikách:

– bezpečné obálky, vytvářené autoritou generující důkazy s použitím symetrických kryptografických technik,

– digitální podpisy vytvářené generátorem důkazu nebo autoritou generující důkaz s použitím asymetrických kryptografických technik.

Mechanismy nepopiratelnosti poskytují protokoly pro výměnu tokenů nepopiratelnosti specifických pro každou službu nepopiratelnosti. Tokeny nepopiratelnosti jsou tvořeny bezpečnými obálkami a/nebo digitálními podpisy a volitelně doplňkovými daty. Tokeny nepopiratelnosti mohou být uloženy jako informace nepopiratelnosti, která může být následně použita stranami, jež jsou ve sporu, nebo rozhodcem k rozhodování ve sporech.

V závislosti na politice nepopiratelnosti účinné pro specifickou aplikaci a právním prostředí, v jehož rámci aplikace pracuje, mohou být pro doplnění informace nepopiratelnosti požadovány dodatečné informace, například:

– důkaz obsahující důvěryhodné vyznačení času, poskytnuté autoritou pro vyznačování času,

– důkaz poskytnutý notářem, který poskytuje záruku týkající se vytvořených dat nebo činnosti či události uskutečněné jednou nebo více entitami.

Nepopiratelnost může být zajištěna pouze v kontextu jasně definované bezpečnostní politiky pro konkrétní aplikaci a její legislativní prostředí. Politiky nepopiratelnosti jsou popsány v ISO/IEC 10181-4.

---

1 Předmět normy

Tato část ISO/IEC 13888 slouží jako obecný model pro následující části specifikující mechanismy nepopiratelnosti používající kryptografické techniky. Tato mezinárodní norma o více částech poskytuje mechanismy nepopiratelnosti pro následující fáze nepopiratelnosti:

– vytváření důkazu,

– přenos, uložení a vyhledávání důkazu a

– ověření důkazu.

Rozhodování sporů leží mimo rozsah této mezinárodní normy.

-- Vynechaný text --