ČESKÁ TECHNICKÁ NORMA

ICS 35.040 **Únor 2012**

Informační technologie – Bezpečnostní techniky – Nepopiratelnost – Část 3: Mechanismy používající asymetrické techniky

ČSN ISO/IEC 13888-3
36 9787

Information technology – Security techniques – Non-repudiation – Part 3: Mechanisms using asymmetric techniques

Technologies de l'information – Techniques de sécurité – Non-répudiation – Partie 3: Mécanismes utilisant des techniques asymétriques

Tato norma je českou verzí mezinárodní normy ISO/IEC 13888-3:2009. Překlad byl zajištěn Úřadem pro technickou normalizaci, metrologii a státní zkušebnictví. Má stejný status jako oficiální verze.

This standard is the Czech version of the International Standard ISO/IEC 13888-3:2009. It was translated by Czech Office for Standards, Metrology and Testing. It has the same status as the official version.

Národní předmluva

Informace o citovaných normativních dokumentech

ISO/IEC 13888-1:2004 nezavedena

ISO/IEC 18014-1:2008 dosud nezavedena

Souvisící ČSN

ČSN ISO 7498-2:1993 (36 9615) Systémy na spracovanie informácií. Prepojenie otvorených systémov (OSI). Základný referenčný model. Část 2: Bezpečnostná architektúra

ČSN ISO/IEC 10118-3:2004 (36 9930) Informační technologie – Bezpečnostní techniky – Hašovací funkce – Část 3: Dedikované hašovací funkce

ČSN ISO/IEC 10118-4:2001 (36 9930) Informační technologie – Bezpečnostní techniky – Hašovací funkce – Část 4: Hašovací funkce používající modulární aritmetiku

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

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

ČSN ISO/IEC TR 14516:2004 (36 9791) Informační technologie – Bezpečnostní techniky – Směrnice pro používání a řízení služeb důvěryhodných třetích stran

ČSN ISO/IEC 15945:2004 (36 9793) Informační technologie – Bezpečnostní techniky – Specifikace služeb TTP na podporu aplikace digitálních podpisů

Vypracování normy

Zpracovatel: Ing. Vladimír Pračke, IČ 40654419

Technická normalizační komise: TNK 42 Výměna dat

Pracovník Úřadu pro technickou normalizaci, metrologii a státní zkušebnictví: Ing. Petr Wallenfels

MEZINÁRODNÍ NORMA

Informační technologie – Bezpečnostní techniky – ISO/IEC 13888-3
Nepopiratelnost – Druhé vydání
Část 3: Mechanismy používající asymetrické techniky 2009-12-15

ICS 35.040

Obsah

Strana

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.org

Web www.iso.org

Published in Switzerland

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 13888-3 byla připravena společnou technickou komisí ISO/IEC JTC 1, *Informační technologie,* subkomise SC 27, *Bezpečnostní techniky IT*.

Druhé vydání zrušuje a nahrazuje první vydání (ISO/IEC 13888-3:1997), které prošlo technickou revizí.

ISO/IEC 13888 se skládá z následujících částí se společným názvem *Informační technologie – Bezpečnostní techniky – 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 validovat 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 je zaměřena pouze na následující služby nepopiratelnosti:

- nepopiratelnost původu,
- nepopiratelnost doručení,
- nepopiratelnost podání,
- nepopiratelnost přenosu.

Takové důkazy mohou být vytvářeny buď přímo koncovou entitou, nebo důvěryhodnou třetí stranou.

Mechanismy nepopiratelnosti zahrnují výměnu tokenů nepopiratelnosti specifických pro každou službu nepopiratelnosti. Mechanismy nepopiratelnosti definované v této části ISO/IEC 13888 sestávají z digitálních podpisů a dodatečných dat.

Tokeny nepopiratelnosti jsou uchovávány jako informace nepopiratelnosti a jsou následně používány v případě sporů.

Pro sestavení tokenu nepopiratelnosti jsou požadovány dodatečné informace. V závislosti na politice nepopiratelnosti, účinné pro specifickou aplikaci, a právním prostředí, v jehož rámci aplikace pracuje, by měly být tyto dodatečná informace v jedné z následujících forem:

- informace poskytovaná autoritou pro vyznačování času, která poskytuje záruku, že podpis tokenu nepopiratelnosti byl vytvořen před stanoveným časem,
- informace poskytovaná službou časových značek, která poskytuje záruku, že podpis tokenu nepopiratelnosti byl zaznamenán před stanoveným časem.

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

1 Předmět normy

Tato část ISO/IEC 13888 specifikuje mechanismy pro poskytování specifických komunikace se týkajících služeb nepopiratelnosti využívajících asymetrické techniky.