ČESKÁ TECHNICKÁ NORMA

ICS 35.040 **Únor 2012**

# Informační technologie – Bezpečnostní techniky – Nepopiratelnost – Část 2: Mechanismy používající symetrické techniky

**ČSN ISO/IEC 13888-2**
36 9787

Information technology – Security techniques – Non-repudiation – Part 2: Mechanisms using symmetric techniques

Technologies de l,information – Techniques de sécurité – Non-répudiation – Partie 2: Mécanismes utilisant des techniques symétriques

Informationstechnik – Sicherheitsverfahren – Nichtabstreitbarkeit – Teil 2: Mechanismen auf Basis von symmetrischen Techniken

Tato norma je českou verzí mezinárodní normy ISO/IEC 13888-2:2010. 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 13888-2:2010. 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 9798-1:1997 nezavedena

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

ISO/IEC 13888-1 zavedena v ČSN ISO/IEC 13888-1 (36 9787) Informační technologie – Bezpečnostní techniky – Nepopiratelnost – Část 1: Všeobecně

Souvisící ČSN

ČSN ISO 7498-2:1993 Systémy na spracovanie informácií – Prepojenie otvorených systémov (OSI) – Základný referenčný model – Časť 2: Bezpečnostná architektúra

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

Další informace

Pro anglický termín „time stamp“ (čl. 3.10) je pro účely této normy použit v souladu s terminologií zavedenou normou ČSN ISO/IEC 18014-1 český termín „vyznačení času“, a s ohledem na běžnou praxi je rovněž uveden další často používaný termín „časové razítko“.

Anglický termín symbol se překládá českým slovem symbol, protože se zde používá ve významu nadřazeného termínu vůči podřazeným termínům: značky, znaky, označení atd., aby se všechny tyto termíny nemusely vypisovat.

Vypracování normy

Zpracovatel: Ing. Vladimír Pračke, IČ 40654419

Technická normalizační komise: TNK 20 Výměna dat

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

MEZINÁRODNÍ NORMA

Informační technologie – Bezpečnostní techniky – ISO/IEC 13888-2
Nepopiratelnost – Druhé vydání
Část 2: Mechanismy používající symetrické techniky 2010-12-15

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 13888-2 byla připravena společnou technickou komisí ISO/IEC JTC 1, *Informační technologie,* subkomise SC 27, *Bezpečnostní techniky IT*.

Toto druhé vydání zrušuje a nahrazuje první vydání (ISO/IEC 13888-2:1998), 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*

## 1 Předmět normy

Cílem služby nepopiratelnosti je vytvářet, shromažďovat, udržovat, zpřístupňovat 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 obecné struktury, které mohou být použity pro služby nepopiratelnosti, a některé specifické mechanismy týkající se komunikace, které mohou být použity pro zajištění služeb nepopiratelnosti původu (NRO) a nepopiratelnosti doručení (NRD). Ostatní služby nepopiratelnosti mohou být vytvořeny použitím obecných struktur popsaných v této části ISO/IEC 13888, aby vyhověly požadavkům definovaným bezpečnostní politikou.

Tato část ISO/IEC 13888 se opírá o existenci důvěryhodné třetí strany (TTP), jejímž účelem je zabránit falešnému popření nebo obvinění. Obvykle je nutná on-line důvěryhodná třetí strana.

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