

# 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

Předmluva 5

Úvod 6

**1** Předmět normy 7

**2** Citované normativní dokumenty 7

**3** Termíny a definice 7

**4** Symboly a zkrácené termíny 7

**5** Požadavky 8

**6** Zapojení důvěryhodné třetí strany 8

**7** Digitální podpisy 9

**8** Použití tokenů nepopiratelnosti s doručovacími autoritami a bez nich 9

**9** Důkazy vytvořené koncovými entitami 9

**9.1** Všeobecně 9

**9.2** Nepopiratelnost původu 10

<b>9.2.1</b>	Token nepopiratelnosti původu (NRO)	10
<b>9.2.2</b>	Mechanismus nepopiratelnosti původu	10
<b>9.3</b>	Nepopiratelnost doručení	11
<b>9.3.1</b>	Token nepopiratelnosti doručení (NRD)	11
<b>9.3.2</b>	Mechanismus pro nepopiratelnosti doručení	11
<b>10</b>	Důkazy vytvořené doručovací autoritou	12
<b>10.1</b>	Všeobecně	12
<b>10.2</b>	Nepopiratelnost podání	12
<b>10.2.1</b>	Token nepopiratelnosti podání (NRS)	12
<b>10.2.2</b>	Mechanismus pro nepopiratelnosti podání	13
<b>10.3</b>	Nepopiratelnost přenosu	13
<b>10.3.1</b>	Token nepopiratelnosti přenosu (NRT)	13
<b>10.3.2</b>	Mechanismus pro nepopiratelnosti přenosu	14
<b>11</b>	Mechanismy zajišťující, že NR token byl podepsán před časem $t$	14
<b>11.1</b>	Všeobecně	14
<b>11.2</b>	Mechanismus používající službu vyznačování času	14
<b>11.3</b>	Mechanismus používající službu časových značek	14
	Bibliografie	16

Odmítnutí odpovědnosti za 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, pokud nejsou typy písma, které jsou vloženy, 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 vytvoření tohoto souboru PDF lze najít ve Všeobecných informacích, které se vztahují k souboru; parametry, na jejichž základě 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, že vznikne problém, který se týká souboru, informujte o tom Ústřední sekretariát ISO na níže uvedené adrese.



**DOKUMENT CHRÁNĚNÝ COPYRIGHTEM**

© ISO/IEC 2009

Veškerá práva vyhrazena. Pokud není specifikováno jinak, nesmí být žádná část této publikace reprodukována nebo používána v jakékoliv formě nebo jakýmkoliv způsobem, elektronickým nebo mechanickým, včetně fotokopíí a mikrofilmů, bez písemného svolení buď od organizace ISO na níže uvedené adrese, nebo od členské organizace ISO 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.org](mailto:copyright@iso.org)

Web [www.iso.org](http://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 zabývajícími 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 dodatečné 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 komunikací se týkajících služeb nepopiratelnosti využívajících asymetrické techniky.

Konec náhledu - text dále pokračuje v placené verzi ČSN.