ČESKÁ TECHNICKÁ NORMA

ICS 35.040

Květen

2001

	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

Informationstechnik - Sicherheitsverfahren - Nichtabstreitbarkeit - Teil 3: Mechanismen auf Basis von asymmetrischen Techniken

Tato norma je českou verzí mezinárodní normy ISO/IEC 13888-3:1997. Mezinárodní norma ISO/IEC 13888-3:1997 má status české technické normy.

This standard is the Czech version of the International Standard ISO/IEC 13888-3:1997. The International Standard ISO/IEC 13888-3:1997 has the status of a Czech Standard.

60916

Národní předmluva

Citované normy

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

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

ISO/IEC 9796:1991, zavedena v ČSN ISO/IEC 9796 (36 9780) Informační technologie - Bezpečnostní techniky - Schémata digitálního podpisu umožňující obnovu zprávy, nahrazena ISO/IEC 9796-3:2000

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

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

ISO/IEC 13888-1:1997, zavedena v ČSN ISO/IEC 13888-1 (36 9787) Informační technologie - Bezpečnostní techniky - Nepopiratelnost - Část 1: Všeobecně

ISO/IEC 14888 (všechny části), dosud nezavedena

Vypracování normy

Zpracovatel: Ing. Vladimír Pračke, IČO 40654419

Technická normalizační komise: TNK 42 Výměna dat

Pracovník Českého normalizačního institutu: Ing. Petr Wallenfels

---

MEZINÁRODNÍ NORMA

Informační technologie - Bezpečnostní techniky - Nepopiratelnost **ISO/IEC 13888-3**

První vydání

1997-12-01

ICS 35.040

Deskriptory: data processing, information interchange, protection of information, security techniques.

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 dotyčnou organizací a zabývajících se určitou oblastí technické činnosti. Technické komise ISO a IEC spolupracují v oblastech společných zájmů. Práce se zúčastňují i mezinárodní komise, vládní i nevládní, s nimiž ISO a IEC navázalo pracovní styk.

ISO a IEC ustavily v oblasti informační technologie společnou technickou komisi, ISO/IEC JTC 1. Návrhy mezinárodních norem, přijaté společnou technickou komisí, se rozesílají národním orgánům k hlasování. Vydání mezinárodní normy vyžaduje souhlas alespoň 75% hlasujících členů.

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

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*

Další části mohou následovat.

Příloha A této části ISO/IEC 13888 je pouze informativní.

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 specifikuje mechanismy pro zajištění některých specifických služeb nepopiratelnosti, týkajících se komunikace a využívajících asymetrické techniky.

Jsou specifikovány mechanismy nepopiratelnosti k ustavení následujících služeb nepopiratelnosti:

– nepopiratelnost původu,

– nepopiratelnost doručení,

– nepopiratelnost podání,

– nepopiratelnost přenosu.

Mechanismy nepopiratelnosti zahrnují výměnu tokenů nepopiratelnosti specifických pro každou službu nepopiratelnosti. Tokeny nepopiratelnosti se skládají z digitálních podpisů a dodatečných dat. Tokeny nepopiratelnosti musí být uloženy jako informace nepopiratelnosti, které mohou být následně použity v případě sporů.

V závislosti na politice nepopiratelnosti, platné pro specifickou aplikaci, a právním prostředí, v rámci kterého aplikace pracuje, mohou být pro zkompletování informace nepopiratelnosti vyžadovány dodatečné informace, např.

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

– důkaz zajiš»ovaný notářem, který poskytuje ujištění o činnosti nebo události, provedené jednou nebo více entitami.

Nepopiratelnost může být zajištěna pouze v rámci kontextu jasně vymezené bezpečnostní politiky pro konkrétní aplikaci a její právní prostředí. Politiky nepopiratelnosti jsou popsány v normě o několika částech Bezpečnostní struktury otevřených systémů - Část 4: Struktura nepopiratelnosti, ISO/IEC 10181-4.

-- Vynechaný text --