ČESKÁ TECHNICKÁ NORMA

ICS 35.040

Květen

2001

	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 13888-2:1998. Mezinárodní norma ISO/IEC 13888-2:1998 má status české technické normy.

This standard is the Czech version of the International Standard ISO/IEC 13888-2:1998. The International Standard ISO/IEC 13888-2:1998 has the status of a Czech Standard.

60674

Národní předmluva

Citované normy

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

ISO/IEC 9797:1994 zavedena v ČSN ISO/IEC 9797 (36 9782) Informační technologie - Bezpečnostní techniky - Mechanismus integrity dat používající kryptografickou kontrolní funkci s využitím algoritmu blokové šifry

ISO/IEC 9798-1:1997 zavedena v ČSN ISO/IEC 9798-1 (36 9743) Informační technologie - Bezpečnostní techniky - Mechanismy autentizace entit - Část 1: Obecný model, nahrazena ISO/IEC 9797-1:1999

ISO/IEC 9798-4:1995 zavedena v ČSN ISO/IEC 9798-4 (36 9743) Informační technologie - Bezpečnostní techniky - Autentizace entit - Část 4: Mechanismy používající kryptografickou kontrolní funkci, nahrazena ISO/IEC 9798-4:1999

ISO/IEC 10118-1:1994 zavedena v ČSN ISO/IEC 10118-1 (36 9930) Informační technologie - Bezpečnostní techniky - Hash funkce - Část 1: Všeobecně, nahrazena ISO/IEC 10118-1:2000

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 13881-1 (36 9787) Informační technologie - Bezpečnostní techniky - Nepopiratelnost - Část 1: Všeobecně

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 -
Část 2: Mechanismy používající symetrické techniky

ISO/IEC 13888-2

První vydání

1998-04-01

ICS 35.040

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

Obsah

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 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 13888-2 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 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 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)*, nepopiratelnosti doručení *(NRD)*, nepopiratelnosti podání *(NRS)* a nepopiratelnosti přenosu *(NRT)*. Ostatní služby nepopiratelnosti mohou být vytvořeny použitím obecných struktur popsaných v kapitole 8, aby vyhověly požadavkům vymezeným bezpečnostní politikou.

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

Mechanismy nepopiratelnosti poskytují protokoly pro výměnu tokenů nepopiratelnosti, specifických pro každou službu nepopiratelnosti. Tokeny nepopiratelnosti používané v této části jsou tvořeny bezpečnými obálkami a dodatečnými daty. Tokeny nepopiratelnosti musí být uloženy jako informace nepopiratelnosti, které mohou být následně použity v případě sporu.

V závislosti na politice nepopiratelnosti, platné pro specifickou aplikaci, a legislativním prostředí, v rámci kterého aplikace pracuje, mohou být pro zkompletování informace nepopiratelnosti vyžadovány dodatečné informace, například:

důkaz zahrnující důvěryhodné vyznačení času poskytované autoritou pro vyznačení 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 ČSN ISO/IEC 10181-4.

-- Vynechaný text --