ČESKÁ TECHNICKÁ NORMA

ICS 35.040

Květen

2001

	Informační technologie - Bezpečnostní techniky - Nepopiratelnost - Část 1: Všeobecně	ČSN ISO/IEC 13888-1 36 9787

Information technology - Security techniques - Non repudiation - Part 1: General

Technologies de l’information - Techniques de sécurité - Non-répudiation - Partie 1: Généralités

Informationstechnik - Sicherheitsverfahren - Nichtabstreitbarkeit - Teil 1: Allgemeines Modell

Tato norma je českou verzí mezinárodní normy ISO/IEC 13888-1:1997. Mezinárodní norma ISO/IEC 13888-1:1997 má status české technické normy.

This standard is the Czech version of the International Standard ISO/IEC 13888-1:1997. The International Standard ISO/IEC 13888-1:1997 has the status of a Czech Standard.

60520

Národní předmluva

Citované normy

ISO 7498-2:1989 zavedena v ČSN ISO 7498-2 (36 9615) Systémy na spracovanie informácií - Prepojenie

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 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, nahrazena ISO/IEC 9797-1:1999

ISO/IEC 10118-1:1994 zavedena v ČSN ISO/IEC 10118-1:1996 (36 9930) Informační technologie - Bezpečnostní techniky - Hash funkce - Část 1: Všeobecně, nahrazena ISO/IEC 10118-1:2000

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 14888 (všechny části) dosud nezavedena

ISO/IEC 11770-3 dosud nezavedena

Upozornění na národní přílohu

Do této normy byla doplněna národní příloha NA, která obsahuje vysvětlivky k textu.

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 13888-1
První vydání
1997-12-01

ICS 35.040

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

Obsah

Strana

1 Předmět normy 6

2 Normativní odkazy 6

3 Definice 7

3.1 Definice z ISO 7498-2 7

3.2 Definice z ISO/IEC 9594-8 7

3.3 Definice z ISO/IEC 10118-1 7

3.4 Definice z ISO/IEC 10181-1 8

3.5 Definice z ISO/IEC 10181-4 8

3.6 Definice z ISO/IEC 11770-3 8

3.7 Definice jedinečné pro tuto normu 8

4 Notace a zkratky 10

5 Požadavky 11

6 Organizace normy 12

7 Generické služby

nepopiratelnosti..... 12

7.1 Entity zúčastněné na zajištění a ověření důkazu..... 12

7.2 Služby nepopiratelnosti 12

8 Zapojení důvěryhodné třetí strany..... 13

8.1 Fáze vytváření důkazu 13

8.2 Fáze přenosu, uložení a vyhledávání důkazu..... 14

8.3 Fáze ověření důkazu 14

9 Mechanismy vytváření a ověřování důkazu..... 14

9.1 Bezpečné obálky 14

9.2 Digitální podpisy 15

9.3 Mechanismus ověřování důkazu..... 15

10 Tokeny nepopiratelnosti 15

10.1 Generický token nepopiratelnosti..... 16

10.2 Token vyznačení času..... 16

10.3 Notarizační token .....

Strana

11 Specifické služby nepopiratelnosti..... 17

11.1 Nepopiratelnost původu..... 18

11.2 Nepopiratelnost doručení..... 18

11.3 Nepopiratelnost podání..... 18

11.4 Nepopiratelnost přenosu..... 19

12 Použití specifických tokenů nepopiratelnosti v prostředí předávání zpráv..... 19

Příloha A (informativní) Bibliografie..... 21

Národní příloha NA (informativní) 22

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 -1 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*

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

---

1 Předmět normy

Cílem služby nepopiratelnosti je vytvářet, shromažďovat, udržovat, zajistit dostupnost 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 model mechanismů nepopiratelnosti poskytujících důkazy, které jsou založeny na kryptografických technikách. Mechanismy nepopiratelnosti, obecně použitelné pro různé služby nepopiratelnosti, jsou nejprve popsány a potom aplikovány na vybrané služby nepopiratelnosti jako:

– nepopiratelnost původu,

– nepopiratelnost doručení,

– nepopiratelnost podání,

– nepopiratelnost přenosu.

Služby nepopiratelnosti zajiš»ují důkaz: důkaz zajiš»uje (jednoznačnou) odpovědnost ve vztahu k jednotlivé události nebo činnosti. Entita odpovědná za danou činnost nebo spojená s danou událostí, vzhledem k níž je generován důkaz, je označována jako subjekt důkazu. Existují dva hlavní typy důkazů, jejichž povaha závisí na použitých kryptografických technikách:

– bezpečné obálky, vytvářené autoritou generující důkazy s použitím symetrických kryptografických technik,

– digitální podpisy vytvářené generátorem důkazů nebo autoritou generující důkazy s použitím asymetrických kryptografických technik.

Mechanismy nepopiratelnosti poskytují protokoly pro výměnu tokenů nepopiratelnosti specifických pro každou službu nepopiratelnosti. Tokeny nepopiratelnosti jsou tvořeny bezpečnými obálkami a/nebo digitálními podpisy a volitelně doplňkovými daty. Tokeny nepopiratelnosti mohou být uloženy jako informace nepopiratelnosti, která může být následně použita stranami, jež jsou ve sporu, nebo rozhodcem k rozhodování ve sporech.

V závislosti na politice nepopiratelnosti účinné pro specifickou aplikaci a právním prostředí, v jehož rámci aplikace pracuje, mohou být pro doplnění informace nepopiratelnosti požadovány dodatečné informace, například:

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

– důkaz poskytnutý notářem, který poskytuje záruku týkající se vytvořených dat nebo činnosti či události uskutečněné jednou nebo více entitami.

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

Tato část ISO/IEC 13888 slouží jako obecný model pro následující části specifikující mechanismy nepopiratelnosti používající kryptografické techniky. ISO/IEC 13888 poskytuje mechanismy nepopiratelnosti pro tyto fáze nepopiratelnosti:

– vytváření důkazu,

– přenos, uložení a vyhledávání důkazu, a

– ověření důkazu.

Rozhodování sporu leží mimo rozsah ISO/IEC 13888.

-- Vynechaný text --