

	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.

© Český normalizační institut,
2001

60674

Podle zákona č. 22/1997 Sb. smějí být české technické normy rozmnožovány
a rozšiřovány jen se souhlasem Českého normalizačního institutu.

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

Strana 3

MEZINÁRODNÍ NORMA

Informační technologie - Bezpečnostní techniky - 13888-2

ISO/IEC

Nepopiratelnost -

První vydání

Část 2: Mechanismy používající symetrické techniky

1998-04-01

ICS 35.040

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

Obsah

Strana

1.....	Předmět normy	
		6
2.....	Normativní odkazy	
		6
3.....	Definice	
		7
4.....	Notace a zkratky	
		7
4.1.....	Notace	
		7
4.1.1.....	Notace z ISO/IEC 13888-1	
	...	7
4.1.2.....	Notace jedinečná pro účely této části ISO/IEC 13888.....	7
4.2.....	Zkratky	
		7
5.....	Požadavky	
		8
6.....	Uspořádání této části ISO/IEC 13888.....	8
7.....	Bezpečné obálky	
		8
8.....	Vytváření a ověřování tokenů nepopiratelnosti.....	9

8.1.....	Vytváření tokenů důvěryhodnou třetí stranou.....	9
8.2.....	Datové položky použité v mechanismech nepopiratelnosti.....	9
8.2.1.....	Datové položky použité v bezpečných obálgách.....	9
8.2.2.....	Datové položky použité v tokenech nepopiratelnosti.....	9
8.3.....	Tokeny nepopiratelnosti	10
8.3.1.....	Token nepopiratelnosti původu	10
8.3.2.....	Token nepopiratelnosti doručení	10
8.3.3.....	Token nepopiratelnosti podání	11
8.3.4.....	Token nepopiratelnosti přenosu	11
8.3.5.....	Token vyznačení času	11
8.4.....	Ověřování tokenů důvěryhodnou třetí stranou.....	12
8.4.1.....	On-line ověřování tokenů	12
8.4.2.....	Tabulka tokenů	12
9.....	Specifické mechanismy nepopiratelnosti.....	

9.1.....	Mechanismus pro nepopiratelnost původu.....	12
9.1.1.....	Transakce 1 - mezi původcem <i>A</i> a <i>TTP</i>	13
9.1.2.....	Transakce 2 - od původce <i>A</i> k příjemci <i>B</i>	13
9.1.3.....	Transakce 3 - mezi příjemcem <i>B</i> a <i>TTP</i>	13

Strana 4

		Strana
9.2.....	Mechanismus pro nepopiratelnost doručení.....	13
9.2.1.....	Transakce 1 - mezi příjemcem <i>B</i> a <i>TTP</i>	13
9.2.2.....	Transakce 2 - od příjemce <i>B</i> k původci <i>A</i>	13
9.2.3.....	Transakce 3 - mezi původcem <i>A</i> a <i>TTP</i>	13
9.3.....	Mechanismus pro nepopiratelnost podání.....	14
9.3.1.....	Transakce 1 - od předkládající entity <i>X</i> k doručovací autoritě <i>DA</i>	14
9.3.2.....	Transakce 2 - od doručovací autority <i>DA</i> k entitě <i>X</i>	14
9.4.....	Mechanismus pro nepopiratelnost přenosu.....	14
9.4.1.....	Transakce 1 - od entity <i>X</i> k doručovací autoritě <i>DA</i>	14
9.4.2.....	Transakce 2 - od doručovací autority <i>DA</i> k entitě <i>Y</i>	14
9.4.3.....	Transakce 3 - od doručovací autority <i>DA</i> k entitě <i>X</i>	14
9.5.....	Mechanismus pro získání tokenu vyznačení	

časů.....	14
9.5.1..... Transakce 1 - od entity <i>X</i> k autoritě pro vyznačování času TSA.....	14
9.5.2..... Transakce 2 - od autority pro vyznačování času TSA k entitě <i>X</i>	15
10..... Příklady mechanismů nepopíratelnosti	15
10.1..... Mechanismus M1: Povinná <i>NRO</i> , volitelná <i>NRD</i>	15
10.1.1... Transakce 1 - mezi původcem <i>A</i> a <i>TTP</i>	16
10.1.2... Transakce 2 - od původce <i>A</i> k příjemci <i>B</i>	16
10.1.3... Transakce 3 - mezi příjemcem <i>B</i> a <i>TTP</i>	16
10.1.4... Transakce 4 - od příjemce <i>B</i> k původci <i>A</i>	16
10.1.5... Transakce 5 - mezi původcem <i>A</i> a důvěryhodnou třetí stranou <i>TTP</i>	16
10.2..... Mechanismus M2: Povinná <i>NRO</i> , povinná <i>NRD</i>	16
10.2.1... Transakce 1 - mezi původcem <i>A</i> a <i>TTP</i>	16
10.2.2... Transakce 2 - od původce <i>A</i> k příjemci <i>B</i>	17
10.2.3... Transakce 3 - mezi příjemcem <i>B</i> a <i>TTP</i>	17
10.2.4... Transakce 4 - mezi <i>TTP</i> a původcem <i>A</i>	17
10.3..... Mechanismus M3: Povinná <i>NRO</i> a <i>NRD</i> se zprostředkující <i>TTP</i>	17
10.3.1... Transakce 1 - mezi původcem <i>A</i> a <i>TTP</i>	18
10.3.2... Transakce 2 - od <i>TTP</i> k příjemci <i>B</i>	18

10.3.3... Transakce 3 - mezi příjemcem <i>B</i> a <i>TTP</i>	18
10.3.4... Transakce 4 - mezi <i>TTP</i> a původcem <i>A</i>	19
Příloha A (informativní) Literatura	20

Strana 5

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.

Strana 6

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 popsanych v kapitole 8, aby vyhovely 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 zajišťovaný 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 --