

**2006**

Informační technologie - Bezpečnostní techniky - Kódy pro autentizaci zprávy (MAC) - Část 2: Mechanismy používající dedikovanou hašovací funkci	ČSN ISO/IEC 9797-2  36 9782
--	--------------------------------------

Information technology - Security techniques - Message Authentication Codes (MACs) -  
Part 2: Mechanisms using a dedicated hash-function

Technologies de l'information - Techniques de sécurité - Codes d'authentification de message (MAC) -  
Partie 2: Mécanismes utilisant une fonction de hachage

Informationstechnik - IT-Sicherheitsverfahren Codes zur Erkennung von Nachrichtenveränderungen  
(MACs) -  
Teil 2: Mechanismen auf Basis einer dedizierten Hash-Funktion

Tato norma je českou verzí mezinárodní normy ISO/IEC 9797-2:2002. Překlad byl zajištěn Českým normalizačním institutem. Má stejný status jako oficiální verze.

This standard is the Czech version of the International Standard ISO/IEC 9797-2:2002. It was translated by Czech Standards Institute. It has the same status as the official version.

The logo of the Czech Standards Institute (ČNI) consists of the letters 'čni' in a stylized, lowercase font, with a grey rectangular bar to the right of the letters.	© Český normalizační institut, 2006 <b>76424</b> Podle zákona č. 22/1997 Sb. smějí být české technické normy rozmnožovány a rozšiřovány jen se souhlasem Českého normalizačního institutu.
---	---

## Národní předmluva

### Informace o citovaných normativních dokumentech

ISO IEC 646:1991 zavedena v ČSN ISO/IEC 646:1995 (36 9104) Informační technika. 7-bitový kódovaný soubor znaků ISO pro výměnu informací

ISO 7498-2:1989 zavedena v ČSN ISO 7498-2:1993 (36 9615) Systémy na spracovanie informácií. Prepojenie otvorených systémov (OSI). Základný referenčný model. Část 2: Bezpečnostná architektúra

ISO/IEC 10118-1:2000 zavedena v ČSN ISO/IEC 10118-1:2002 (36 9930) Informační technologie - Bezpečnostní techniky - Hašovací funkce - Část 1: Všeobecně

ISO/IEC 10118-3:1998 zavedena v ČSN ISO/IEC 10118-3:2004 (36 9930) Informační technologie - Bezpečnostní techniky - Hašovací funkce - Část 3: Dedikované hašovací funkce

### Vypracování normy

Zpracovatel: Ing. Vladimír Pračke, IČ 40654419

Technická normalizační komise: TNK 20 Informační technologie

Pracovník Českého normalizačního institutu: Ing. Petr Wallenfels

Strana 3

---

#### Odmítavé stanovisko k 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, ledaže by typy písma, které jsou vloženy, byly 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 nepřejímá za její porušení žádnou odpovědnost.

Adobe je obchodní značka „Adobe Systems Incorporated“.

Podrobnosti o softwarových produktech použitých k vytváření tohoto souboru PDF, lze najít ve Všeobecných informacích, které jsou k souboru připojeny; parametry, pomocí kterých 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, tj. když vznikne problém, který se týká souboru, informujte o tom na níže uvedené adrese Ústřední sekretariát ISO.

© ISO/IEC 2002

Všechna práva vyhrazena. ©ádná část této normy nesmí být reprodukována nebo zpracována jakoukoliv jinou formou, jako například elektronickou, mechanickou, včetně fotokopíí a mikrofilmu bez

písemného povolení ISO. Povolení lze vyžádat na níže uvedené adrese nebo u členské národní organizace v zemi žadatele.

ISO copyright office

Case postale 56, CH-1211 Geneva 20

Tel. +41 22 749 01 11

Fax. +41 22 734 10 79

e-mail [copyright@iso.ch](mailto:copyright@iso.ch)

Web [www.iso.ch](http://www.iso.ch)

Strana 4

---

Prázdná strana

Strana 5

---

## **MEZINÁRODNÍ NORMA**

Informační technologie - Bezpečnostní techniky -

Kódy pro autentizaci zprávy (MAC) -

Část 2: Mechanismy používající dedikovanou hašovací funkci

ISO/IEC 9797-2

První vydání

2002-06-01

ICS 35.040

Obsah

	Strana
<b>1</b> Předmět normy .....	8
<b>2</b> Normativní odkazy .....	8
<b>3</b> Termíny a definice .....	8

<b>4</b>	Symboly a zápis	
	.....	
	10	
<b>5</b>	Požadavky	
	.....	
	..... 11	
<b>6</b>	MAC algoritmus	
	1.....	
	11	
<b>6.1</b>	Popis MAC algoritmu	
	1.....	12
<b>6.1.1</b>	Krok 1 (expanze klíče).....	
	12	
<b>6.1.2</b>	Krok 2 (modifikace konstant a IV).....	12
<b>6.1.3</b>	Krok 3 (hašovací operace).....	12
<b>6.1.4</b>	Krok 4 (výstupní transformace).....	
	12	
<b>6.1.5</b>	Krok 5 (zkrácení)	
	.....	
	12	
<b>6.2</b>	Výkonnost	
	.....	
	..... 13	
<b>6.3</b>	Výpočet konstant	
	.....	
	13	
<b>6.3.1</b>	Dedikovaná hašovací funkce	
	1.....	13
<b>6.3.2</b>	Dedikovaná hašovací funkce	
	2.....	14
<b>6.3.3</b>	Dedikovaná hašovací funkce	

3.....	14
<b>7</b> MAC algoritmus	
2.....	
14	
<b>7.1</b> Popis MAC algoritmu	
2.....	15
<b>7.1.1</b> Krok 1 (expanze klíče).....	
15	
<b>7.1.2</b> Krok 2 (hašovací operace).....	15
<b>7.1.3</b> Krok 3 (výstupní transformace).....	
15	
<b>7.1.4</b> Krok 4 (zkrácení) .....	
15	
<b>7.2</b> Výkonnost .....	
..... 15	
<b>8</b> MAC algoritmus	
3.....	
15	
<b>8.1</b> Popis MAC algoritmu	
3.....	16
<b>8.1.1</b> Krok 1 (expanze klíče).....	
16	
<b>8.1.2</b> Krok 2 (modifikace konstant a IV).....	16
<b>8.1.3</b> Krok 3 (doplnění) .....	
16	
<b>8.1.4</b> Krok 4 (aplikace funkce zaokrouhlení).....	16
<b>8.1.5</b> Krok 5	

(zkrácení)

.....  
17

## 8.2

Výkonnost

.....  
..... 17

## Příloha A (informativní)

Příklady.....  
18

## Příloha B (informativní) Bezpečnostní analýza MAC

algoritmů..... 22

Strana 6

---

### 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 zabývajících 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 3 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 této části ISO/IEC 9797 mohou být předmětem patentových práv. ISO a IEC nelze považovat za odpovědné za identifikování některých nebo všech takových patentových práv.

ISO/IEC 9797-2 byla připravena společnou technickou komisí ISO/IEC JTC 1, *Informační technologie, subkomise SC 27, Bezpečnostní techniky IT*.

ISO/IEC 9797 se skládá z následujících částí se společným názvem *Informační technologie - Bezpečnostní techniky - Kódy pro autentizaci zprávy (MACs)*:

- Část 1: *Mechanismy používající blokové šifry*
- Část 2: *Mechanismy používající dedikované hašovací funkce*

Další části mohou následovat.

Přílohy A a B této části ISO/IEC 9797 jsou pouze informativní.

## Úvod

ISO (Mezinárodní organizace pro normalizaci) a IEC (Mezinárodní elektrotechnická komise) upozorňují na skutečnost, že se tvrdí, že vyhovění této části ISO/IEC 9797 může zahrnovat použití patentového práva týkajícího se MAC Algoritmu 1 (MDx-MAC) uvedeného v kapitole 6.

ISO a IEC nezaujímají stanovisko k evidenci, platnosti a rozsahu tohoto patentového práva.

Držitel tohoto patentového práva ubezpečil ISO a IEC, že je ochoten se za rozumných a nediskriminujících podmínek a požadavků dohodnout s jakýmkoliv žadatelem na licencích. Prohlášení držitele tohoto patentového práva je v této souvislosti u ISO a IEC zaznamenáno. Informace lze získat od

Entrust Technologies, Technology Licensing Dept., 750 Heron Road, Ottawa, Ontario, Canada K1V 1A7.

Pozornost je nutno věnovat možnosti, že některé prvky této části ISO/IEC 9797 mohou být předmětem patentových práv jiných než výše uvedených. ISO a IEC nelze považovat za odpovědné za identifikování některých nebo všech takových patentových práv.

# 1 Předmět normy

Tato část ISO/IEC 9797 specifikuje tři algoritmy MAC, které používají tajný klíč a hašovací funkci (nebo její funkci zaokrouhlení) s  $n$ -bitovým výsledkem pro výpočet  $m$ -bitového MAC. Tyto mechanismy mohou být použity jako mechanismy integrity dat k ověření, že data nebyla změněna neautorizovaným způsobem. Mohou být rovněž použity jako mechanismy pro autentizaci zprávy poskytující záruku, že zpráva byla vytvořena entitou vlastnící tajný klíč. Síla mechanismu integrity dat a autentizace zprávy závisí na délce (v bitech)  $k$  a utajení klíče, na délce (v bitech)  $n$  hašovacího kódu vytvořeného hašovací funkcí, na síle hašovací funkce, na délce (v bitech)  $m$  kódu MAC a na specifickém mechanismu.

Tři mechanismy specifikované v této části ISO/IEC 9797 jsou založeny na dedikovaných hašovacích funkcích specifikovaných v ISO/IEC 10118-3. První mechanismus specifikovaný v této části ISO/IEC 9797 je všeobecně znám jako MDx-MAC. Volá celou hašovací funkci jednou, ale provádí drobnou modifikaci funkce zaokrouhlení přidáním klíče k aditivním konstantám funkce zaokrouhlení. Druhý mechanismus specifikovaný v této části ISO/IEC 9797 je všeobecně znám jako HMAC. Volá celou hašovací funkci dvakrát. Třetí mechanismus specifikovaný v této části ISO/IEC 9797 je variantou MDx-MAC, která používá na vstupu pouze krátké řetězce (nanejvýš 256 bitů). Poskytuje vyšší výkon aplikacím, které pracují pouze s krátkými vstupními řetězci.

Tato část ISO/IEC 9797 může být aplikována na služby bezpečnosti libovolné architektury, procesu nebo aplikace bezpečnosti.