ČESKÁ TECHNICKÁ NORMA

ICS 35.040 **Srpen**
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 oficielní 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.

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

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

Web www.iso.ch

Prázdná strana

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

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.

-- Vynechaný text --