ČESKÁ TECHNICKÁ NORMA

ICS 35.040 **Červenec 2013**

Informační technologie – Bezpečnostní techniky – Kódy pro autentizaci zprávy (MACs) – 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 dédiée

Tato norma je českou verzí mezinárodní normy ISO/IEC 9797-2:2011 Corrected version 2011-06. Překlad byl zajištěn Úřadem pro technickou normalizaci, metrologii a státní zkušebnictví. Má stejný status jako oficiální verze.

This standard is the Czech version of the International Standard ISO/IEC 9797-2:2011 Corrected version 2011-06. It was translated by the Czech Office for Standards, Metrology a Testing. It has the same status as the official version.

Národní předmluva

Informace o citovaných dokumentech

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

Souvisící ČSN

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

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

ČSN ISO/IEC 9797-1:2013 (36 9782) Informační technologie – Bezpečnostní techniky – Kódy pro autentizaci zprávy (MACs) – Část 1: Mechanismy používající blokovou šifru

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

ČSN ISO/IEC 10181-6:1999 (36 9694) Informační technologie – Propojení otevřených systémů –

Bezpečnostní struktury otevřených systémů: Struktura integrity

Vypracování normy

Zpracovatel: Ing. Alena Hönigová, IČ 61470716

Technická normalizační komise: TNK 20 Informační technologie

Pracovník Úřadu pro technickou normalizaci, metrologii a státní zkušebnictví: Ing. Petr Wallenfels

MEZINÁRODNÍ NORMA

Informační technologie – Bezpečnostní techniky – ISO/IEC 9797-2
Kódy pro autentizaci zprávy (MACs) – První vydání
Část 2: Mechanismy používající dedikovanou hašovací funkci 2011-05
Druhé vydání Opravená verze
2011-06

ICS 35.040

Obsah

Strana

Published in Switzerland

Předmluva

ISO (Mezinárodní organizace pro normalizaci) a IEC (Mezinárodní elektrotechnická komise) tvoří specializovaný systém celosvětové normalizace. Národní orgány, které jsou členy ISO nebo IEC, se podílejí na vypracování mezinárodních norem prostřednictvím technických komisí ustavených příslušnými organizacemi pro jednotlivé obory technické činnosti. Technické komise ISO a IEC spolupracují v oborech společného zájmu. Práce se zúčastňují také další vládní a nevládní mezinárodní organizace, s nimiž ISO a IEC navázaly pracovní styk. V oblasti informační technologie zřídily ISO a IEC společnou technickou komisi ISO/IEC JTC 1.

Návrhy mezinárodních norem jsou vypracovávány v souladu s pravidly danými směrnicemi ISO/IEC, část 2.

Hlavním úkolem společné technické komise je vypracování mezinárodních norem. Návrhy mezinárodních norem přijaté společnou technickou komisí jsou rozesílány národním členům k hlasování. Vydání mezinárodní normy vyžaduje souhlas alespoň 75 % hlasujících národních orgánů.

ISO/IEC 9797-2 vypracovala společná technická komise ISO/IEC JTC 1 *Informační technologie,* subkomise 27 *Bezpečnostní techniky IT.*

Toto druhé vydání zrušuje a nahrazuje první vydání (ISO/IEC 9797-2:2002), které bylo technicky revidováno přidáním algoritmů MAC založených na dedikovaných hašovacích funkcích 4 – 7 z ISO/IEC 10118-3:2004 a dedikované hašovací funkce 8 z ISO/IEC 10118-3/Amd.1:2006.

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

- Část 1: Mechanismy používající blokovou šifru
- Část 2: Mechanismy používající dedikovanou hašovací funkci
- Část 3: Mechanismy používající univerzální hašovací funkci

Mohou následovat další části.

Tato opravená verze ISO/IEC 9797-2:2011 začleňuje opravy 3.14, 6.3, 6.3.5 a 6.3.6.

Úvod

Mezinárodní organizace pro normalizaci (ISO) a Mezinárodní elektrotechnická komise (IEC) upozorňuje na to, že je třeba věnovat pozornost skutečnosti, že vyhovění této části ISO/IEC 9797 může zahrnovat použití patentu týkajícího se algoritmu 1 MAC (MDx-MAC) uvedeného v kapitole 6.

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

Držitel tohoto patentového práva ujistil ISO a IEC, že je ochoten dohodnout s uživateli na celém světě licence za rozumných a nediskriminačních okolností a podmínek. V tomto ohledu je prohlášení držitele tohoto patentového práva registrováno u ISO a IEC. Informace lze získat u společnosti:

> Entrust Technologies, Technology Licensing Dept., 1000 Innovation Drive, Ottawa, Ontario, Canada K2K 3E7.

Pozornost je věnována možnosti, že některé prvky tohoto dokumentu mohou být předmětem jiných patentových práv než těch, které jsou uvedeny výše. ISO a IEC nepřebírají zodpovědnost za identifikaci jakýchkoliv 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 zaokrouhlovací funkci) s *n*-bitovým výsledkem k výpočtu *m*-bitového MAC. Tyto mechanismy mohou být použity jako mechanismy integrity dat k ověření, že tato data nebyla změněna neautorizovaným způsobem. Mohou být také použity jako mechanismy pro autentizaci zprávy k poskytnutí záruky, že zpráva byla vytvořena entitou, která vlastní tajný klíč. Síla mechanismů integrity dat a autentizace zprávy závisí na entropii a utajení klíče, na délce (v bitech) *n* hašovacího kódu vytvořeného hašovací funkcí, na síle hašovací funkce, na délce (v bitech) *m* MAC a na konkrétním mechanismu.

Tři mechanismy specifikované v této části ISO/IEC 9797 jsou založeny na dedikovaných hašovacích funkcích specifikovaných v ISO/IEC 10118-3. První mechanismus se nazývá MDx-MAC. Volá hašovací funkci jednou, ale provádí malou modifikaci zaokrouhlovací funkce v hašovací funkci přičtením klíče k aditivním konstantám v zaokrouhlovací funkci. Druhý mechanismus se nazývá HMAC. Volá hašovací funkci dvakrát. Třetí mechanismus je variantou MDx-MAC, který má jako vstup pouze krátké řetězce (nejvíce 256 bitů). Nabízí vyšší výkon u aplikací, které pracují pouze s krátkými vstupními řetězci dat.

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

POZNÁMKA Všeobecný rámec pro zajištění služeb integrity je specifikován v ISO/IEC 10181-6 [5].