ČESKÁ TECHNICKÁ NORMA

ICS 35.040 **Březen 2016**

# Informační technologie – Bezpečnostní techniky – Kódy pro autentizaci zprávy (MAC) – Část 3: Mechanismy používající univerzální hašovací funkci

ČSN
ISO/IEC 9797-3
36 9782

Information technology – Security techniques – Message Authentication Codes (MACs) – Part 3: Mechanisms using a universal hash-function

Technologies de l,information – Techniques de sécurité – Codes d,authentification de message (MAC) –
Partie 3: Mécanismes utilisant une fonction de hachage universelle

Tato norma je českou verzí mezinárodní normy ISO/IEC 9797-3:2011. 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 9797-3:2011. It was translated by the Czech Office for Standards, Metrology and Testing. It has the same status as the official version.

Národní předmluva

Informace o citovaných dokumentech

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

ISO/IEC 18031 dosud nezavedena

ISO/IEC 18033-3 dosud nezavedena

ISO/IEC 18033-4 dosud nezavedena

Souvisící ČSN

ČSN ISO/IEC 10181-6 (36 9694) Informační technologie – Propojení otevřených systémů – Bezpečnostní struktury otevřených systémů: Struktura integrity

Vysvětlivky k textu převzaté normy

Pro účely této normy byl použit překlad anglického termínu „tag“ jako „označení“.

Následující anglické termíny byly použity v původním tvaru, vzhledem k rozšíření těchto termínů v odborné

komunitě a/nebo absenci českého ekvivalentu:

Nonce, Badger.

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. Miroslav Škop

MEZINÁRODNÍ NORMA

Informační technologie – Bezpečnostní techniky – ISO/IEC 9797-3
Kódy pro autentizaci zprávy (MAC) – První vydání
Část 3: Mechanismy používající univerzální hašovací funkci 2011-11-15

ICS 34.050

Obsah

Strana

ISO copyright office

Case postale 56 · CH-1211 Geneva 20

Tel. + 41 22 749 01 11

Fax + 41 22 749 09 47

E-mail copyright@iso.org

Web www.iso.org

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 svých technických komisí ustavených příslušnými organizacemi pro jednotlivé obory technické činnosti. Technické komise ISO a IEC spolupracují v oblastech společných zájmů. 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 technickými komisemi se rozesílají národním orgánům k hlasování. Vydání mezinárodní normy vyžaduje souhlas alespoň 75 % hlasujících národních orgánů.

Upozorňuje se na možnost, že některé prvky tohoto dokumentu mohou být předmětem patentových

práv. ISO a IEC nelze činit odpovědnými za identifikování jakéhokoliv nebo všech patentových práv.

ISO/IEC 9797-3 vypracovala společná technická komise ISO/IEC JTC 1 *Informační technologie,* subkomise SC 27 *IT Bezpečnostní techniky*.

ISO/IEC 9797 se společným názvem *Informační technologie – Bezpečnostní techniky – Kódy pro autentizaci zprávy (MAC)* se sestává z těchto samostatných částí:

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

Úvod

V prostředí IT je často požadováno, aby bylo možné ověřit, že elektronická data nebyla změněna neautorizovaným způsobem a že je možné poskytnout záruku, že zpráva byla vytvořena entitou, která vlastní tajný klíč. Algoritmus MAC (Message Authentication Code (Kód pro autentizaci zprávy)) je obecně používaným mechanismem zajišťujícím integritu, který může splňovat tyto požadavky.

Tato část ISO/IEC 9797 specifikuje čtyři algoritmy MAC používající univerzální hašovací funkce: UMAC, Badger, Poly1305-AES a GMAC.

Tyto mechanismy mohou být použity jako mechanismy zajišťující integritu dat k ověření, že 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 mechanismu pro integritu dat a mechanismu pro autentizaci zprávy závisí na délce (v bitech) a utajení klíče, na délce (v bitech) hašovacího kódu vytvořeného hašovací funkcí, na síle hašovací funkce, na délce (v bitech) MAC, a na konkrétním mechanismu.

POZNÁMKA Obecný rámec pro poskytnutí služeb integrity je specifikován v ISO/IEC 10181-6[7].

1 Předmět normy

Tato část ISO/IEC 9797 specifikuje následující algoritmy MAC, které používají tajný klíč a univerzální hašovací funkci s *n*-bitovým výsledkem k výpočtu *m*-bitového MAC na základě blokových šifer specifikovaných v ISO/IEC 18033-3 a proudových šifer specifikovaných v ISO/IEC 18033-4:

a. UMAC;
b. Badger;
c. Poly1305-AES;
d. GMAC.