ČESKÁ TECHNICKÁ NORMA

ICS 35.040 **Červen 2013**

Informační technologie – Bezpečnostní techniky – Kódy pro autentizaci zprávy (MACs) – Část 1: Mechanismy používající blokovou šifru

ČSN ISO/IEC 9797-1
36 9782

Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher

Technologies de l,information – Techniques de sécurité – Codes d,authentification de message (MAC) – Partie 1: Mécanismes utilisant un chiffrement par blocs

Tato norma je českou verzí mezinárodní normy ISO/IEC 9797-1:2011. 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 9797-1:2011. 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 18033-3 dosud nezavedena

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 8825-1:2012 (36 9635) Informační technologie – Pravidla kódování ASN.1: Specifikace základních pravidel kódování (BER), kanonických pravidel kódování (CER) a rozlišujících pravidel kódování (DER)

ČSN ISO/IEC 9798-1:2011 (36 9743) Informační technologie – Bezpečnostní techniky – Autentizace entit – Část 1: Všeobecně

Vypracování normy

Zpracovatel: Ing. Alena Hönigová, IČO 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 9797-1
Kódy pro autentizaci zprávy (MACs) – Druhé vydání
Část 1: Mechanismy používající blokovou šifru 2011-03

ICS 35.040

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 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.

Upozorňuje se na možnost, že některé prvky tohoto dokumentu mohou být předmětem patentových práv. ISO a IEC nelze činit odpovědnými za identifikaci jakéhokoliv nebo všech patentových práv.

ISO/IEC 9797-1 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 9797-1:1999), které bylo technicky revidováno. Algoritmy 5 a 6 MAC z ISO/IEC 9797-1:1999, které se skládaly ze dvou jednotlivých výpočtů CBC-MAC, byly nahrazeny dvěma dalšími algoritmy MAC, které provádějí jednotlivé výpočty CBC-MAC a které nabízejí zvýšenou efektivnost. Byla přidána příloha A o identifikátorech objektů. Bezpečnostní analýza v příloze C byla aktualizována a byla přidána příloha D o vztahu k předchozím normám.

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.

Úvod

V prostředí IT je často požadováno, aby bylo možné ověřit, že elektronická data nebyla neautorizovaně změněna, a aby bylo možné poskytnout záruku, že zpráva pochází od entity, která vlastní tajný klíč. Algoritmus MAC (Message Authentication Code – Kód pro autentizaci zprávy) je obecně používaný mechanismus pro zajištění integrity dat, který může tyto požadavky splňovat.

Tato část ISO/IEC 9797 specifikuje šest algoritmů MAC založených na n-bitové blokové šifře. Vypočítávají krátký řetězec jako funkci tajného klíče a zprávy proměnné délky.

Síla mechanismu integrity dat a mechanismu autentizace zprávy je závislá na délce (v bitech) k^* a utajení klíče, na délce bloku (v bitech) n a síle blokové šifry, na délce (v bitech) m algoritmu MAC, a na konkrétním mechanismu.

První mechanismus specifikovaný v této části ISO/IEC 9797 se nazývá CBC-MAC (CBC je zkratka pro Cipher Block Chaining).

Dalších pět mechanismů jsou varianty CBC-MAC. Algoritmy 2, 3, 5 a 6 MAC používají na konci zpracování speciální transformaci. Algoritmus 6 MAC je optimalizovanou variantou algoritmu 2 MAC. Algoritmus 5 MAC používá minimální počet šifrování. Algoritmus 5 MAC vyžaduje pouze systém šifrovacího klíče pro jednu blokovou šifru, ale potřebuje delší interní klíč. Algoritmus 4 MAC používá speciální transformaci na začátku i na konci zpracování; tento algoritmus je doporučen k použití v aplikacích, které požadují, aby délka klíče algoritmu MAC byla dvojnásobkem délky klíče blokové šifry.

1 Předmět normy

Tato část ISO/IEC 9797 specifikuje šest algoritmů MAC, které používají k výpočtu m-bitového MAC tajný klíč a n-bitovou blokovou šifru.

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

Mechanismy správy klíčů jsou mimo rozsah této části ISO/IEC 9797.

Tato část ISO/IEC 9797 specifikuje identifikátory objektů, které mohou být použity v souladu s ISO/IEC 8825-1 k identifikaci každého mechanismu. Jsou uvedeny číselné příklady a bezpečnostní analýza každého ze šesti specifikovaných algoritmů, a je objasněn vztah této části ISO/IEC 9797 k dřívějším normám.