

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 and 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

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

Předmluva 6

Úvod 7

1 Předmět normy 8

2 Citované dokumenty 8

3 Termíny a definice 8

4 Symboly a značení 9

5 Požadavky 10

6 Model pro algoritmy MAC 11

6.1 Obecně 11

6.2 Krok 1 (odvození klíče) 12

6.2.1 Obecně 12

6.2.2 Metoda 1 pro odvození klíče 12

6.2.3 Metoda 2 pro odvození klíče 12

6.3 Krok 2 (doplnění) 13

6.3.1 Obecně 13

6.3.2 Metoda doplnění 1 13

6.3.3 Metoda doplnění 2 13

6.3.4 Metoda doplnění 3 13

6.3.5 Metoda doplnění 4 13

6.4	Krok 3 (rozdělení)	13
6.5	Krok 4 (iterace)	14
6.6	Krok 5 (závěrečná iterace)	14
6.6.1	Obecně	14
6.6.2	Závěrečná iterace 1	14
6.6.3	Závěrečná iterace 2	14
6.6.4	Závěrečná iterace 3	14
6.7	Krok 6 (výstupní transformace)	14
6.7.1	Obecně	14
6.7.2	Výstupní transformace 1	14
6.7.3	Výstupní transformace 2	14
6.7.4	Výstupní transformace 3	15
6.8	Krok 7 (zkrácení)	15
7	Algoritmy MAC	15
7.1	Obecně	15
7.2	Algoritmus 1 MAC	15
7.3	Algoritmus 2 MAC	15
7.4	Algoritmus 3 MAC	16
7.5	Algoritmus 4 MAC	17
7.6	Algoritmus 5 MAC	18
7.7	Algoritmus 6 MAC	19
Příloha A	(normativní) Identifikátory objektů	21
Příloha B	(informativní) Příklady	23
B.1	Obecně	23
B.2	Algoritmus 1 MAC	24
B.3	Algoritmus 2 MAC	25
B.4	Algoritmus 3 MAC	26

B.5 Algoritmus 4 MAC 27

B.6 Algoritmus 5 MAC 30

B.6.1 Příklady procesu generování MAC 30

B.6.2 AES používající 128-bitový klíč 30

B.6.3 AES používající 192-bitový klíč 30

B.6.4 AES používající 256-bitový klíč 31

B.6.5 Triple DEA s trojitým klíčem 31

B.6.6 Triple DEA s dvojitým klíčem 31

B.7 Algoritmus 6 MAC 32

B.7.1 Příklady procesu generování MAC 32

B.7.2 AES používající 128-bitový klíč 32

B.7.3 AES používající 192-bitový klíč 32

B.7.4 AES používající 256-bitový klíč 33

Příloha C (informativní) Bezpečnostní analýza algoritmů MAC 34

C.1 Obecně 34

C.2 Zdůvodnění 35

Příloha D (informativní) Porovnání s předchozími normami algoritmů MAC 41

Bibliografie 42

Odmítnutí odpovědnosti za 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, pokud nejsou typy písma, které jsou vloženy, 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 nepřijímá za její porušení žádnou odpovědnost.

Adobe je obchodní značka „Adobe Systems Incorporated“.

Podrobnosti o softwarových produktech použitých k vytvoření tohoto souboru PDF lze najít ve Všeobecných informacích, které se vztahují k souboru; parametry, na jejichž základě byl PDF soubor vytvořen, byly optimalizovány pro tisk. Soubor byl zpracován s maximální péčí tak, aby ho členská organizace ISO mohly používat. V málo pravděpodobném případě, že vznikne problém, který se týká souboru, informujte o tom Ústřední sekretariát ISO na níže uvedené adrese.



DOKUMENT CHRÁNĚNÝ COPYRIGHTEM

© ISO/IEC 2011

Veškerá práva vyhrazena. Pokud není specifikováno jinak, nesmí být žádná část této publikace reprodukována nebo používána v jakékoliv formě nebo jakýmkoliv způsobem, elektronickým nebo mechanickým, včetně fotokopíí a mikrofilmů, bez písemného svolení buď od organizace ISO na níže uvedené adrese, nebo od členské organizace ISO v zemi žadatele.

ISO copyright office

Case postale 56 · CH-1211 Geneva 20

Tel. + 41 22 749 01 11

Fax + 41 22 749 09 47

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.

Konec náhledu - text dále pokračuje v placené verzi ČSN.