ČESKÁ TECHNICKÁ NORMA

ICS 35.040

Červenec

2001

	Informační technologie - Bezpečnostní techniky - Kódy pro autentizaci zprávy (MAC) - 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 (MACs) -
Partie 1: Mécanismes utilisant un cryptogramme bloc

Informationstechnik - Sicherheitsverfahren - Codes zur Authentifikation von Instanzen - Teil 1: Mechanismen auf Basis eines Blockschlüssel-Algorithmus

Tato norma je českou verzí mezinárodní normy ISO/IEC 9797-1:1999. Mezinárodní norma ISO/IEC 9797-1:1999 má status české technické normy.

This standard is the Czech version of the International Standard ISO/IEC 9797-1:1999. The International
Standard ISO/IEC 9797-1:1999 has the status of a Czech Standard.

61396

Národní předmluva

Citované normy

ISO 7498-2:1989 zavedena v ČSN ISO 7498 (36 9615) Systémy na spracovanie informácií - Prepojenie otvorených systémov (OSI). Základný referenčný model - Časť 2: Bezpečnostná architektúra

ISO/IEC 9798-1 zavedena v ČSN ISO/IEC 9798-1:1998 (36 9743) Informační technologie - Bezpečnostní techniky - Mechanizmy autentizace entit - Část 1: Všeobecně

ISO/IEC 10116:1997 zavedena v ČSN ISO/IEC 10116:1999 (36 9742) Informační technologie - Módy činnosti pro n-bitovou blokovou šifru

Vypracování normy

Zpracovatel: Ing. Alena Hönigová, IČO 61470716

Technická normalizační komise: TNK 42 Výměna dat

Pracovník Českého normalizačního institutu: Ing. Petr Wallenfels

---

MEZINÁRODNÍ NORMA
Informační technologie - Bezpečnostní techniky - Kódy pro autentizaci zprávy (MAC) - Část 1: Mechanismy používající blokovou šifru

ISO/IEC 9797-1
První vydání
1999-12-15

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 a 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 mezinárodní komise, vládní i nevládní, s nimiž ISO a IEC navázalo pracovní styk.

Mezinárodní normy jsou navrhovány v souladu s pravidly obsaženými ve Směrnicích ISO/IEC, Část 3.

ISO a IEC ustavily v oblasti informační technologie společnou technickou komisi, ISO/IEC JTC 1. Návrhy mezinárodních norem, přijaté společnou technickou komisí, se rozesílají národním orgánům k hlasování. Vydání mezinárodní normy vyžaduje souhlas alespoň 75% hlasujících členů.

Mezinárodní norma ISO/IEC 9797-1 byla připravena společnou technickou komisí ISO/IEC JTC 1, *Informační technologie,* subkomise SC 27, *Bezpečnostní techniky IT.*

První vydání ISO/IEC 9797-1 spolu s dalšími částmi ISO/IEC 9797 ruší a nahrazuje ISO/IEC 9797:1994, která byla předmětem revize a byla rozšířena na normu o více částech. Implementace, které odpovídají ISO/IEC 9797:1994 však budou ve shodě s tímto vydáním 9797-1.

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

– *Část 1: Mechanismy používající blokovou šifru*

– *Část 2: Mechanismy používající hašovací funkci*

Mohou následovat další části.

Přílohy A a B této části ISO/IEC 9797 jsou pouze informativní.

---

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. Tyto mechanismy mohou být použity jako mechanismy integrity dat pro ověření, že data nebyla změněna neautorizovaným způsobem. Mohou být také použity jako mechanismy pro autentizaci zprávy, k poskytnutí záruky, že zpráva pochází od entity vlastnící tajný klíč. Síla mechanismu integrity dat a mechanismu autentizace zprávy závisí na délce *k** (v bitech) a na utajení klíče, na délce bloku *n* (v bitech) a na síle blokové šifry, na délce *m* (v bitech) kódu MAC a na specifickém mechanismu.

První tři mechanismy specifikované v této části ISO/IEC 9797 se obecně nazývají CBC-MAC (CBC je zkratka Cipher Block Chaining). Výpočet MAC, tak jak je popsán v ISO 8731-1 a ANSI X9.9, je specifickým případem této části ISO/IEC 9797, kde $n = 64$, $m = 32$ a jsou použity algoritmus MAC 1 a metoda doplnění 1 a bloková šifra je DEA (ANSI X3.92:1981). Výpočet MAC popsaný v ANSI X9.19 a ISO 9807 je specifickým případem této části ISO/IEC 9797, kde $n = 64$, $m = 32$, je použit buďto algoritmus MAC 1 nebo algoritmus MAC 3 (oba s metodou doplnění 1) a bloková šifra je DEA (ANSI X3.92:1981).

Čtvrtý mechanismus je variantou CBC MAC se speciální počáteční transformací. Je doporučen pro aplikace, které vyžadují, aby délka klíče algoritmu MAC byla dvojnásobnou délkou blokové šifry.

POZNÁMKY

1 Například v případě DEA (ANSI X3.92:1981) je délka klíče blokové šifry 56 bitů, zatímco délka klíče algoritmu MAC je 112 bitů.

2 Jestliže je algoritmus používán s DEA (známým také jako DES), nazývá se MacDES [12].

Pátý a šestý mechanismus používá dvě paralelní instance prvního a čtvrtého mechanismu a kombinuje tyto dva výsledky s exclusive-or operacemi prováděnými po bitech. Jsou doporučeny pro aplikace, které vyžadují zvýšenou úroveň bezpečnosti proti útokům padělání (viz přílohu B). Pátý mechanismus používá jednoduchou délku klíče algoritmu MAC, zatímco šestý mechanismus délku klíče algoritmu MAC zdvojnásobuje.

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

-- Vynechaný text --