ČESKÁ NORMA

ICS 03.060

Leden 1996

# Bankovnictví - Schválené algoritmy pro autentizaci zprávy - část 2: Algoritmus autentikátora zprávy

**ČSN**
**ISO 8731-2**

97 9003

Banking - Approved algorithms for message authentication - Part 2: Message authenticator algorithm

Banque - Algorithmes approuvés pour l'authentification des messages - Partie 2: Algorithme d'authentification des messages

Bankwesen - Billigte Algorithmen für Berichtsbeglaubigung Teil 2: Algorithmus des Berichtsbeglaubigers

Tato norma je identická s ISO 8731-2:1992, druhé vydání.

**Národní předmluva**

**Citované normy**

ISO 7185:1990  dosud nezavedena

ISO 8730 zavedena v ČSN ISO 8730 Bankovnictví - Požadavky na autentizaci zprávy (bankovní služby pro velkou klientelu) (97 9008)

**Vypracování normy**

Zpracovatel: Ing. Dagmar Jírová, IČO 18651399

Technická normalizační komise: TNK 42 Výměna dat

Pracovník Českého normalizačního institutu: Ing. Petr Wallenfels

**Bankovnictví - Schválené algoritmy pro autentizaci zprávy - 2. část: Algoritmus autentikátora zprávy**

**ISO 8731-2**
**Druhé vydání**
**1992-09-15**

**Obsah** strana



## Předmluva

ISO (Mezinárodní organizace pro normalizaci) je celosvětovou federací národních normalizačních organizací (členů ISO). Na mezinárodních normách obvykle pracují technické komise ISO. Každý člen ISO, který se zajímá o předmět, pro který byla vytvořena technická komise, má právo být zastoupen v této technické komisi. Práce se zúčastňují i mezinárodní organizace, vládní i nevládní, s nimiž ISO navázalo pracovní styk. ISO úzce spolupracuje s Mezinárodní technickou komisí (IEC) ve všech záležitostech normalizace v elektrotechnice.

Návrhy mezinárodních norem přijaté technickými komisemi se rozesílají členům ISO k hlasování. Vydání mezinárodní normy vyžaduje souhlas alespoň 75 % z hlasujících členů.

Mezinárodní norma ISO 8731-2 byla připravena technickou komisí ISO/TC 68 Bankovnictví a související finanční služby, subkomisí SC2, Operace a postupy.

Toto druhé vydání ruší a nahrazuje první vydání (ISO 8731-2: 1987), jehož je technickou revizí.

ISO 8731 se skládá z následujících částí, pod společným názvem Bankovnictví - Schválené algoritmy pro autentizaci zprávy:

- Část 1: DEA
- Část 2: Algoritmus autentikátora zprávy

Přílohy A a B této části mezinárodní normy ISO 8731 mají pouze informativní charakter.

## 1 Předmět normy

ISO 8731 specifikuje v jednotlivých částech schválený algoritus autentizace, tj. schválený v tom smyslu, že splňuje autentizační požadavky ISO 8730. Tato část ISO 8731 se zabývá algoritmem autentikátora zprávy vzhledem k jeho využití při výpočtu Kódu autentizace zprávy (MAC).

Algoritmus autentikátora zprávy (MAA) je specificky vyvinut pro velmi rychlou autentizaci při využití sálového (mainframe) počítače. Je to algoritmus se speciálním použitím v případech velkého objemu dat a je-li požadována efektivní softwarová implementace. MAA je rovněž vhodný při použití programovatelného kalkulátoru.

Testovací příklady jsou uvedeny v příloze A, která není součástí této části ISO 8731. Další testovací příklad je uveden jako příloha v ISO 8730.

Specifikace MAA ve VDM je uvedena v příloze B, která není součástí této části ISO 8731.

---

**-- Vynechaný text --**