



**BANKOVNICTVÍ -
Schválené algoritmy pro autentizaci
zprávy
- Část 1: DEA**

Leden 1996

**ČSN
ISO 8731-1**

97 9003

Banking - Approved algorithms for message authentication - Part 1: DEA

Banque - Algorithmes approuvés pour l'authentification des messages - Partie 1: DEA

Bankwesen - Billigte Algorithmen für Berichtsbeglaubigung Teil 1: DEA

Tato norma je identická s ISO 8731-1:1987, první vydání.

Národní předmluva

Citované normy

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

ANSI X3.92-1981 dosud nezavedena

ANSI X3.106-1983 dosud nezavedena

ANSI X9.9-1982 dosud nezavedena

POZNÁMKA - Normy ANSI jsou dostupné v Českém normalizačním institutu, úsek informatiky, Praha 1, Václavské náměstí 19.

Vypracování normy

Zpracovatel: Ing. Dagmar Jírová, IČO 18651399

Technická normalizační komise: TNK 42 Výměna dat

**BANKOVNICTVÍ - SCHVÁLENÉ ALGORITMY
PRO AUTENTIZACI ZPRÁVY
Část 1: DEA**

**ISO 8731-1
První vydání
1987-06-01**

Deskriptory: banking, banking documents, messages, data processing, authentication

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 navázali pracovní styk.

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

Mezinárodní norma ISO 8731-1 byla připravena technickou komisí ISO/TC 68, *Bankovníctví*.

Úvod

ISO 8731 specifikuje v samostatných částech schválené autentizační algoritmy. Každý algoritmus je schválen, pokud splňuje autentizační požadavky specifikované v ISO 8730.

1 Předmět normy a oblast užití

Tato část ISO 8731 pojednává o DEA (Data Encryption Algorithm) jako metodě, určené k použití při výpočtu MACu (Message Authentication Code).

Může být implementován softwarově, avšak hardwarová implementace DEA pracuje při podstatně vyšších rychlostech.

-- Vynechaný text --