ČESKÁ NORMA

ICS 03.060;35.240.40

Únor 1996

**Bankovnictví**
**ŘÍZENÍ A BEZPEČNOST OSOBNÍCH IDENTIFIKAČNÍCH ČÍSEL**
**Část 2: Schválené algoritmy pro šifrování PIN**

**ČSN**
**ISO 9564-2**

97 9007

Banking - Personal Identification Number management and security Part 2: Approved algorithm(s) for PIN encipherment

Banque - Gestion et sécurité du numéro personnel d'identification Partie 2: Algorithme(s) approuvé(s) pour le chiffrement du PIN

Bankwesen: PIN-Ausgabe und -Verwaltung und PIN-Sicherheit Teil 2: Anerkannte Algorithmen zur PIN-Verschlüsselung

Tato norma je identická s ISO 9564-2:1991

**Národní předmluva**

**Citované normy**

ISO 8732:1988 dosud nezavedena

ISO 9564-1:1991 Bankovnictví - Řízení a bezpečnost osobních identifikačních čísel. Část 1: Principy a techniky ochrany PIN (97 9007)

ANSI X3.92:1981 dosud nezavedena

**Vypracování normy**

Zpracovatel normy: Česká národní banka, Ing. Alena Hönigová, IČO: 48136450

Technická normalizační komise: TNK 42 Výměna dat

Pracovník Českého normalizačního institutu: Ing. Petr Walllenfells

**Bankovnictví**
**ŘÍZENÍ A BEZPEČNOST OSOBNÍCH IDENTIFIKAČNÍCH ČÍSEL.**
**Část 2: Schválené algoritmy pro šifrování PIN**

**ISO 9564-2**
**První vydání**
**1991-12-15**

MDT 336.717:351.755.6:003.26

Deskriptory: banking, bank accounts, identification methods, registration number, protection of information, coded representation, algorithms.

## Předmluva

ISO (Mezinárodní organizace pro normalizaci) je celosvětovou federací národních normalizačních orgánů (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 elektrotechnickou 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 9564-2 byla připravena technickou komisí ISO/TC 68, *Bankovnictví a související finanční služby*, SC 6, *Finanční transakční karty, související média a operace.*

ISO 9564 sestává z následujících částí pod společným názvem *Bankovnictví - Řízení a bezpečnost osobního identifikačního čísla:*

- *1. část: Principy a techniky ochrany PIN*

- *2. část: Schválený algoritmus(y) pro šifrování PIN*

**Úvod**

Tato část ISO 9564 specifikuje algoritmy schválené pro šifrování osobních identifikačních čísel (PIN). Každý algoritmus je schválen pokud splňuje požadavky na šifrování specifikované v ISO 9564-1. Touto částí ISO 9564 je současně pokryt následující algoritmus:

Algoritmus pro šifrování dat (Data Encryption Algorithm (DEA))

## 1 Předmět normy

Tato část ISO 9564 specifikuje algoritmy schválené pro šifrování osobních identifikačních čísel (PIN).

---

**-- Vynechaný text --**