NORME INTERNATIONALE

ISO 9564-2

Première édition
1991-12-15

Banque — Gestion et sécurité du numéro personnel d'identification —

Partie 2:
Algorithme(s) approuvé(s) pour le chiffrement du PIN

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

Numéro de référence
ISO 9564-2:1991(F)

Avant-propos

L'ISO (Organisation internationale de normalisation) est une fédération mondiale d'organismes nationaux de normalisation (comités membres de l'ISO). L'élaboration des Normes internationales est en général confiée aux comités techniques de l'ISO. Chaque comité membre intéressé par une étude a le droit de faire partie du comité technique créé à cet effet. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO participent également aux travaux. L'ISO collabore étroitement avec la Commission électrotechnique internationale (CEI) en ce qui concerne la normalisation électrotechnique.

Les projets de Normes internationales adoptés par les comités techniques sont soumis aux comités membres pour vote. Leur publication comme Normes internationales requiert l'approbation de 75 % au moins des comités membres votants.

La Norme internationale ISO 9564-2 a été élaborée par le comité technique ISO/TC 68, *Banque et services financiers liés aux opérations bancaires*, sous-comité SC 6, *Cartes de transactions financières, supports et opérations relatifs à celles-ci*.

L'ISO 9564 comprend les parties suivantes, présentées sous le titre général *Banque — Gestion et sécurité du numéro personnel d'identification*:

— *Partie 1: Principes et techniques de protection du PIN*

— *Partie 2: Algorithme(s) approuvé(s) pour le chiffrement du PIN*

Organisation internationale de normalisation
Case Postale 56 • CH-1211 Genève 20 • Suisse

Imprimé en Suisse

Introduction

La présente partie de l'ISO 9564 prescrit les algorithmes approuvés pour le chiffrement des numéros personnels d'identification (PIN). Chaque algorithme est approuvé comme répondant aux prescriptions de chiffrement spécifiées dans l'ISO 9564-1. L'algorithme suivant est actuellement couvert par la présente partie de l'ISO 9564:

Data Encryption Algorithm (DEA)

Page blanche

Banque — Gestion et sécurité du numéro personnel d'identification —

Partie 2:
Algorithme(s) approuvé(s) pour le chiffrement du PIN

1 Domaine d'application

La présente partie de l'ISO 9564 prescrit les algorithmes approuvés pour le chiffrement des numéros personnels d'identification (PIN).

2 Références normatives

Les normes suivantes contiennent des dispositions qui, par suite de la référence qui en est faite, constituent des dispositions valables pour la présente partie de l'ISO 9564. Au moment de la publication, les éditions indiquées étaient en vigueur. Toute norme est sujette à révision et les parties prenantes des accords fondés sur la présente partie de l'ISO 9564 sont invitées à rechercher la possibilité d'appliquer les éditions les plus récentes des normes indiquées ci-après. Les membres de la CEI et de l'ISO possèdent le registre des Normes internationales en vigueur à un moment donné.

ISO 8372:1987, *Traitement de l'information — Modes opératoires d'un algorithme de chiffrement par blocs de 64 bits.*

ISO 9564-1:1991, *Banque — Gestion et sécurité du numéro personnel d'identification — Partie 1: Principes et techniques de protection du PIN.*

ANSI X3.92:1981, *Data Encryption Algorithm (DEA).*

3 Définition de l'algorithme DEA

La définition du DEA doit être celle publiée dans la norme nationale américaine ANSI X3.92:1981.

4 Spécification de l'algorithme DEA

Le chiffrement, au moyen du DEA, des blocs de PIN décrits dans l'ISO 9564-1 doit être réalisé en utilisant l'algorithme fonctionnant dans le mode ECB (Electronic Code Book), décrit dans l'ISO 8372.

Page blanche

Page blanche

CDU 336.717:351.755.6:003.26

Descripteurs: banque, compte bancaire, méthode d'identification, numéro d'immatriculation, protection de l'information, combinaison de code, algorithme.

Prix basé sur 1 page