INTERNATIONAL STANDARD

**ISO 9564-2**

First edition
1991-12-15

# 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*

Reference number
ISO 9564-2:1991(E)

## Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

International Standard ISO 9564-2 was prepared by Technical Committee ISO/TC 68, *Banking and related financial services*, Sub-Committee SC 6, *Financial transaction cards, related media and operations*.

ISO 9564 consists of the following parts, under the general title *Banking — Personal Identification Number management and security*:

— *Part 1: PIN protection principles and techniques*

— *Part 2: Approved algorithm(s) for PIN encipherment*

International Organization for Standardization
Case Postale 56 • CH-1211 Genève 20 • Switzerland

Printed in Switzerland

## Introduction

This part of ISO 9564 specifies algorithms approved for the encipherment of Personal Identification Numbers (PINs). Every algorithm is approved as meeting the encipherment requirements specified in ISO 9564-1. The following algorithm is currently covered by this part of ISO 9564:

Data Encryption Algorithm (DEA)

This page intentionally left blank

# Banking — Personal Identification Number management and security —

## Part 2:
Approved algorithm(s) for PIN encipherment

## 1 Scope

This part of ISO 9564 specifies algorithms approved for the encipherment of Personal Identification Numbers (PINs).

## 2 Normative references

The following standards contain provisions which, through reference in this text, constitute provisions of this part of ISO 9564. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this part of ISO 9564 are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below. Members of IEC and ISO maintain registers of currently valid International Standards.

ISO 8372:1987, *Information processing — Modes of operation for a 64-bit block cipher algorithm.*

ISO 9564-1:1991, *Banking — Personal Identification Number management and security — Part 1: PIN protection principles and techniques.*

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

## 3 Definition of the DEA algorithm

The definition of DEA shall be as published in the American National Standard ANSI X3.92:1981.

## 4 Specification of the DEA algorithm

Encipherment, using DEA, of the PIN blocks described in ISO 9564-1 shall be achieved using the algorithm operating in the Electronic Code Book (ECB) mode, as described in ISO 8372.

This page intentionally left blank

This page intentionally left blank

**UDC 336.717:351.755.6:003.26**

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

Price based on 1 page