INTERNATIONAL STANDARD

ISO 9564-2

Second edition
2005-02-01

Banking — Personal Identification Number management and security —

Part 2: Approved algorithms for PIN encipherment

Banque — Gestion et sécurité du numéro personnel d'identification (PIN) —

Partie 2: Algorithmes approuvés pour le chiffrement du PIN

Reference number
ISO 9564-2:2005(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. 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.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO 9564-2 was prepared by Technical Committee ISO/TC 68, *Financial services*, Subcommittee SC 2, *Security management and general banking operations*.

This second edition cancels and replaces the first edition (ISO 9564-2:1991), which has been technically revised.

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

— *Part 1: Basic principles and requirements for online PIN handling in ATM and POS systems*

— *Part 2: Approved algorithms for PIN encipherment*

— *Part 3: Requirements for offline PIN handling in ATM and POS systems*

— *Part 4: Guidelines for PIN handling in open networks*

Banking — Personal Identification Number management and security —

Part 2: Approved algorithms for PIN encipherment

1 Scope

This part of ISO 9564 specifies algorithms for the encipherment of Personal Identification Numbers (PINs). These algorithms, based on the approval processes established in ISO 9564-1, are the data encryption algorithm (DEA) and the RSA encryption algorithm.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 9564-1, *Banking — Personal Identification Number (PIN) management and security — Part 1: Basic principles and requirements for online PIN handling in ATM and POS systems*

ISO 9564-3, *Banking — Personal Identification Number management and security — Part 3: Requirements for offline PIN handling in ATM and POS systems*

ISO/IEC 10116, *Information technology — Security techniques — Modes of operation for an n-bit block cipher*

ISO 11568-2:1994, *Banking — Key management (retail) — Part 2: Key management techniques for symmetric ciphers*

EMV 2000, *Integrated Circuit Card Specifications for Payment Systems, Book 2: Security and Key Management*[1)]

ANSI INCITS 92-1981, *Data Encryption Algorithm* [formerly ANSI X3.92-1981 (R1998)][2)]

ANSI X9.52-1998, *Triple Data Encryption Algorithm Modes of Operation*[2)]

AS 2805.5.3-1992, *Electronic funds transfer — Requirements for interfaces — Ciphers — Data encipherment algorithm 2 (DEA 2)* [3)]

1) EMV: Europay, Mastercard, VISA.

2) American National Standards Institute standard.

3) Standards Australia standard.

3 Data Encryption Algorithm (DEA)

3.1 Definition

The definition of DEA shall be in accordance with that published in ANSI X3.92:1981.

3.2 Specification

Encipherment, using the TDEA, of the PIN blocks according to ISO 9564-1 shall be achieved using the algorithm operating in the Electronic Code Book (ECB) mode (with n equal to 64) in accordance with ISO/IEC 10116. Each TDEA encryption/decryption operation is a compound operation of DEA encryption/decryption operations, as defined in ISO 11568-2 and ANS X9.52.

4 RSA encryption algorithm

4.1 Definition

The definition of the RSA[4)] encryption algorithm shall be in accordance with that published in AS 2805.5.3:1992.

4.2 Specification

Encipherment, using RSA, of the PIN blocks according to ISO 9564-3 shall be achieved in accordance with EMV 2000, Book 2.

4.3 Applicability

This algorithm is approved for use with ISO 9564-3 only.

4) Named after its inventors, Ronald Rivest, Adi Shamir and Leonard Adleman.

ICS 35.240.40

Price based on 2 pages