INTERNATIONAL STANDARD

ISO 9564-2

Third edition
2014-08-01

Financial services — Personal Identification Number (PIN) management and security —

Part 2: Approved algorithms for PIN encipherment

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

Partie 2: Algorithmes approuvés pour le chiffrement du PIN

Reference number
ISO 9564-2:2014(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

Contents

Page

Foreword ..... **iv**

Introduction ..... **v**

1 Scope **1**

2 Normative references **1**

3 Triple Data Encryption Algorithm (TDEA) **1**
3.1 Definition of the TDEA algorithm 1
3.2 Use of the TDEA algorithm 1

4 RSA encryption algorithm **1**
4.1 Definition of the RSA algorithm 1
4.2 Use of the RSA algorithm 2

5 AES encryption algorithm **2**
5.1 Definition of the AES algorithm 2
5.2 Use of the AES algorithm 2

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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/TC 68, *Financial services*, Subcommittee SC 2, *Financial services, security*.

This third edition cancels and replaces the second edition (ISO 9564-2:2005), which has been technically revised.

ISO 9564 consists of the following parts, under the general title *Financial services — Personal Identification Number (PIN) management and security*:

— *Part 1: Basic principles and requirements for PINs in card-based systems*

— *Part 2: Approved algorithms for PIN encipherment*

— *Part 4: Requirements for PIN handling in eCommerce for payment transactions*

Introduction

This part of ISO 9564 specifies algorithms approved for the encipherment of Personal Identification Numbers (PINs). The following algorithms, based on the approval processes established in ISO 9564-1, are:

— Triple Data Encryption Algorithm (TDEA);

— RSA;

— Advanced Encryption Standard (AES).

Financial services — Personal Identification Number (PIN) management and security —

Part 2: Approved algorithms for PIN encipherment

1 Scope

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

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. 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, *Financial services – Personal Identification Number management and security – Part 1: Basic principles and requirements for PINs in card-based systems*

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

ISO/IEC 18033-2, *Information technology – Security techniques – Encryption algorithms – Part 2: Asymmetric ciphers*

ISO/IEC 18033-3, *Information technology – Security techniques – Encryption algorithms – Part 3: Block ciphers*

3 Triple Data Encryption Algorithm (TDEA)

3.1 Definition of the TDEA algorithm

The definition of TDEA shall be as described in the ISO/IEC 18033-3.

3.2 Use of the TDEA algorithm

Encipherment, using the TDEA as described in ISO/IEC 18033-3 with TDEA keying option 1 or 2, of the PIN blocks described in ISO 9564-1 shall be achieved using the algorithm operating in the Electronic Code Book (ECB) mode (with *n* equal to 64), as described in ISO/IEC 10116.

This algorithm is approved for use with PIN block formats 0, 1, and 3 only.

4 RSA encryption algorithm

4.1 Definition of the RSA algorithm

The definition of RSA shall be as described in ISO/IEC 18033-2.

4.2 Use of the RSA algorithm

The format 2 PIN block and its encipherment, using RSA, shall be as described in ISO 9564-1.

This algorithm is approved only for use for encipherment of offline PINs for submission to ICCs as defined in ISO 9564-1. It is approved for use with PIN block format 2 only.

5 AES encryption algorithm

5.1 Definition of the AES algorithm

The definition of AES shall be as described in ISO/IEC 18033-3.

5.2 Use of the AES algorithm

Encipherment, using AES as described in ISO/IEC 18033-3, of the PIN blocks described in ISO 9564-1 shall be achieved using the algorithm operating in the Electronic Code Book (ECB) mode (with block size *n* equal to 128), as described in ISO/IEC 10116.

This algorithm is approved for use with PIN block format 4 only.