
**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

get full document from standards.iteh.ai



Sample Document

get full document from standards.iteh.ai



COPYRIGHT PROTECTED DOCUMENT

© ISO 2014

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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

Sample Document

get full document from standards.iteh.ai

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).

Sample Document

get full document from standards.iteh.ai