International Standard

ISO 9564-2

Fourth edition

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

PROOF/ÉPREUVE

Reference number
ISO 9564-2:2025(en)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

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 document 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).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents. ISO shall not be held responsible for identifying any or all such patent rights.

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

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 68 *Financial services*, Subcommittee SC 2, *Financial services, security*.

This fourth edition cancels and replaces the third edition (ISO 9564-2:2014), which has been technically revised.

The main changes are as follows:

— in this revision, Rivest-Shamir-Adleman algorithm (RSA) can be also be used for PIN encryption during PIN issuance and change over open networks;

— SM4 has been added as an additional 16-byte block cipher;

— ECIES has been added as an option for offline PIN encryption to an IC card;

— a new appendix has been added to provide guidance on using asymmetric techniques to transport an ephemeral symmetric PIN encryption key.

A list of all parts in the ISO 9564 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.