INTERNATIONAL STANDARD

**ISO 9564-1**

Fourth edition
2017-11

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

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

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

*Partie 1: Principes de base et exigences relatifs aux PINs dans les systèmes à carte*

Reference number
ISO 9564-1:2017(E)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

# 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 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 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 the following URL: 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 9564-1:2011), which has been technically revised.

It also incorporates the Amendment ISO 9564-1:2011/Amd 1:2015.

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

# Introduction

A Personal Identification Number (PIN) is used in financial services as one method of cardholder verification.

The objective of PIN management is to protect the PIN against unauthorized disclosure, compromise and misuse throughout its life cycle and, in so doing, to minimize the risk of fraud occurring within electronic funds transfer (EFT) systems. The secrecy of the PIN needs to be ensured at all times during its life cycle, which consists of its establishment, issuance, activation, storage, entry, transmission, validation, deactivation and any other use made of it.

In this document, the following terms are used for the types of communication of the PIN.

a) Conveyance: reference PIN to the integrated circuit (IC) card or cardholder selected PIN to the issuer.

b) Delivery: PIN to the cardholder.

c) Transmission: transaction PIN to the issuer or IC reader for subsequent PIN verification.

d) Submission: transaction PIN to the ICC.

PIN security in part depends upon sound key management. Maintaining the secrecy of cryptographic keys is of the utmost importance because the compromise of any key allows the compromise of any PIN ever enciphered under it.

PINs can be verified online or offline. Since online PIN verification can be performed independent of the card itself, any type of payment card or device can be used to initiate such a transaction. However, there are special card requirements for those cards that perform offline PIN verification on the card itself.

Financial transaction cards with embedded IC can support offline PIN verification using the IC of the card. Issuers can choose whether to have PIN verification performed online or offline. Offline PIN verification does not require that a cardholder's PIN be sent to the issuer host for verification and so security requirements relating to PIN protection differ from online PIN verification security requirements. However, many general PIN protection principles and techniques are still applicable even though a PIN can be verified offline.

This document is designed so that issuers can achieve reasonable assurance that a PIN, while under the control of other institutions, is properly managed. Techniques are given for protecting the PIN-based customer authentication process by safeguarding the PIN against unauthorized disclosure during the PIN’s life cycle.

In ISO 9564-2, approved encipherment algorithms for use in the protection of the PIN are specified.

ISO 9564 is one of several series of International Standards which describe requirements for security in the retail banking environment; these include ISO 11568 (all parts), ISO 13491 (all parts) and ISO 16609.

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

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

## 1 Scope

This document specifies the basic principles and techniques which provide the minimum security measures required for effective international PIN management. These measures are applicable to those institutions responsible for implementing techniques for the management and protection of PINs during their creation, issuance, usage and deactivation.

This document is applicable to the management of cardholder PINs for use as a means of cardholder verification in retail banking systems in, notably, automated teller machine (ATM) systems, point-of-sale (POS) terminals, automated fuel dispensers, vending machines, banking kiosks and PIN selection/change systems. It is applicable to issuer and interchange environments.

The provisions of this document are not intended to cover:

a) PIN management and security in environments where no persistent cryptographic relationship exists between the transaction-origination device and the acquirer, e.g. use of a browser for online shopping (for these environments, see ISO 9564-4);

b) protection of the PIN against loss or intentional misuse by the customer;

c) privacy of non-PIN transaction data;

d) protection of transaction messages against alteration or substitution;

e) protection against replay of the PIN or transaction;

f) specific key management techniques;

g) offline PIN verification used in contactless devices;

h) requirements specifically associated with PIN management as it relates to multi-application functionality in an ICC.

## 2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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/IEC 7816 (all parts), *Identification cards — Integrated circuit cards*

ISO 9564-2, *Financial services — Personal Identification Number (PIN) management and security — Part 2: Approved algorithms for PIN encipherment*

ISO 11568 (all parts), *Banking — Key management (retail)*