
**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*

[ISO 9564-1:2017](https://standards.iteh.ai/catalog/standards/iso/75b2020c-13f0-4ea5-b32f-9740a5b275e0/iso-9564-1-2017)

<https://standards.iteh.ai/catalog/standards/iso/75b2020c-13f0-4ea5-b32f-9740a5b275e0/iso-9564-1-2017>



iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

[ISO 9564-1:2017](https://standards.iteh.ai/catalog/standards/iso/75b2020c-13f0-4ea5-b32f-9740a5b275e0/iso-9564-1-2017)

<https://standards.iteh.ai/catalog/standards/iso/75b2020c-13f0-4ea5-b32f-9740a5b275e0/iso-9564-1-2017>



COPYRIGHT PROTECTED DOCUMENT

© ISO 2017, Published in Switzerland

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
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	v
Introduction	vi
1 Scope	1
2 Normative references	1
3 Terms and definitions	2
4 Basic principles of PIN management	5
4.1 General.....	5
4.2 Principles.....	5
5 PIN handling devices	6
5.1 PIN handling device security requirements.....	6
5.2 Physical security for IC readers.....	7
5.3 PIN entry device characteristics.....	7
5.3.1 Character set.....	7
5.3.2 Character representation.....	7
6 PIN security issues	7
6.1 PIN control requirements.....	7
6.1.1 PIN processing systems.....	7
6.1.2 Recording media.....	8
6.1.3 Oral communications.....	8
6.1.4 Telephone keypads.....	8
6.2 PIN encipherment.....	8
7 PIN verification	9
7.1 General.....	9
7.2 Online PIN verification.....	9
7.3 Offline PIN verification.....	9
8 Techniques for management/protection of account-related PIN functions	9
8.1 PIN length.....	9
8.2 PIN establishment.....	9
8.2.1 PIN establishment techniques.....	9
8.2.2 Assigned derived PIN.....	9
8.2.3 Assigned random PIN.....	10
8.2.4 Customer-selected PIN.....	10
8.3 PIN issuance and delivery to the cardholder.....	10
8.4 PIN selection.....	10
8.4.1 General.....	10
8.4.2 PIN conveyance.....	10
8.4.3 PIN selection at an issuer's location.....	11
8.4.4 PIN selection by mail.....	11
8.5 PIN change.....	11
8.5.1 General.....	11
8.5.2 PIN change in an interchange environment.....	11
8.5.3 PIN change at an attended terminal.....	11
8.5.4 PIN change at an unattended terminal.....	12
8.5.5 PIN change by mail.....	12
8.6 PIN replacement.....	12
8.6.1 Replacement of forgotten PIN.....	12
8.6.2 Re-advice of forgotten PIN.....	12
8.6.3 Replacement of compromised PIN.....	12
8.7 Disposal of waste material and returned PIN mailers.....	12
8.8 PIN activation.....	12
8.9 PIN storage.....	13

8.10	PIN deactivation.....	13
8.11	PIN mailers.....	13
9	Techniques for management/protection of transaction-related PIN functions.....	14
9.1	PIN entry.....	14
9.2	Protection of PIN during transmission.....	14
9.2.1	PIN protection during transmission to the issuer for online PIN verification.....	14
9.2.2	PIN protection during conveyance to the ICC for offline PIN verification.....	15
9.3	Compact PIN block formats.....	17
9.3.1	PIN block construction and format value assignment.....	17
9.3.2	Format 0 PIN block.....	17
9.3.3	Format 1 PIN block.....	18
9.3.4	Format 2 PIN block.....	18
9.3.5	Format 3 PIN block.....	19
9.3.6	Compact PIN block usage restrictions.....	20
9.4	Extended PIN blocks.....	21
9.4.1	General.....	21
9.4.2	Format 4 PIN block.....	21
9.5	PIN block format translation restrictions.....	25
9.6	Journalizing of transactions containing PIN data.....	25
Annex A (normative) Destruction of sensitive data.....		26
Annex B (informative) Additional guidelines for the design of a PIN entry device.....		28
Annex C (informative) Information for customers.....		31
Bibliography.....		32

iTech Standards
 (https://standards.iteh.ai)
 Document Preview

ISO 9564-1:2017

<https://standards.iteh.ai/catalog/standards/iso/75b2020c-13f0-4ea5-b32f-9740a5b275e0/iso-9564-1-2017>

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.