



BSI Standards Publication

Financial services — Personal identification number (PIN) management and security

Part 5: Methods for the generation, change, and verification of PINs

National foreword

This British Standard is the UK implementation of ISO 9564-5:2025.

The UK participation in its preparation was entrusted to Technical Committee IST/12, Financial services.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

© The British Standards Institution 2025
Published by BSI Standards Limited 2025

ISBN 978 0 539 26200 1

ICS 35.240.40

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 October 2025.

Amendments/corrigenda issued since publication

Date	Text affected
------	---------------



International
Standard

ISO 9564-5

**Financial services — Personal
identification number (PIN)
management and security —**

**Part 5:
Methods for the generation, change,
and verification of PINs**

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

*Partie 5: Méthodes pour la génération, la modification et la
vérification des PIN*

**First edition
2025-10**

Reference number
ISO 9564-5:2025(en)

Full document details: BS ISO 9564-5:2025

© ISO 2025  **Documents**
Document Sharing Hub



COPYRIGHT PROTECTED DOCUMENT

© ISO 2025

All rights reserved. Unless otherwise specified, or required in the context of its implementation, 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
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	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Symbols and reference terms	3
5 Basic principles	3
5.1 General	3
5.2 PIN management methods	4
5.2.1 PIN offset method	4
5.2.2 PVV method	4
5.2.3 Stored encrypted reference PIN	5
5.2.4 Approved cryptographic algorithms	5
6 PIN generation	5
6.1 General	5
6.2 Random PIN generation method	5
6.3 Deterministic PIN generation method with PIN offset	6
6.3.1 Introduction	6
6.3.2 Method A	6
6.3.3 Method B	7
6.4 PIN offset calculation method	7
7 PIN change	8
7.1 Authentication	8
7.2 Forgotten PIN	8
8 Transaction PIN verification	8
8.1 General	8
8.2 PVV method	9
8.2.1 General	9
8.2.2 Forming the input data	9
8.2.3 Calculating the PIN check value (PVV)	11
8.3 Offset method	11
Annex A (informative) Worked examples	12
Annex B (informative) Mathematical support for calculations	15
Annex C (normative) Base conversion decimalization method	17
Annex D (normative) Scanning decimalization method	19
Bibliography	21

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*.

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.

Introduction

This document specifies requirements and recommendations for cryptographic methods for the generation, change and verification of PINs.

This document has been prepared so that institutions involved in financial services activities wishing to implement PIN management functions can do so in a manner that is secure and facilitates interoperability between separate implementations.

This document identifies ciphers and algorithms from ISO/IEC 18033-3 and ISO/IEC 9797 that are specifically approved for secure banking purposes.

Financial services — Personal identification number (PIN) management and security —

Part 5: Methods for the generation, change, and verification of PINs

1 Scope

This document specifies cryptographic methods for:

- PIN generation;
- reference PIN change;
- transaction PIN verification.

These PIN management functions can be implemented using:

- encryption using an approved algorithm (see [Table 1](#));
- CMAC using an approved block cipher (see [Table 1](#));
- HMAC using an approved hash algorithm (see [Table 1](#)).

Refer to ISO 9564-1 for basic principles & requirements regarding PIN establishment.

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 9564-1, *Financial services — Personal Identification Number (PIN) management and security — Part 1: Basic principles and requirements for PINs in card-based systems*

ISO/IEC 9797-1:2011, *Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher*

ISO/IEC 9797-2:2021, *Information security — Message authentication codes (MACs) — Part 2: Mechanisms using a dedicated hash-function*

ISO 11568, *Financial services — Key management (retail)*

ISO/IEC 18031, *Information technology — Security techniques — Random bit generation*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at <https://www.iso.org/obp>
- IEC Electropedia: available at <https://www.electropedia.org/>