

ISO 9564-2:2025(en)

ISO/TC 68/SC 2

Secretariat: BSI

Date: 2025-06-10

**Financial services — Personal identification number (PIN) management and security — Part 2:
Approved algorithms for PIN encipherment**

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

[ISO/PRF 9564-2](https://standards.iteh.ai/catalog/standards/iso/ef04a57c-3afe-45af-a9eb-97807179a987/iso-prf-9564-2)

<https://standards.iteh.ai/catalog/standards/iso/ef04a57c-3afe-45af-a9eb-97807179a987/iso-prf-9564-2>

© 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

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

ISO/PRF 9564-2

<https://standards.iteh.ai/catalog/standards/iso/ef04a57c-3afe-45af-a9eb-97807179a987/iso-prf-9564-2>

Contents

Foreword.....	iv
Introduction.....	v
1 Scope	1
2 Normative references	1
3 Terms and definitions.....	1
4 General	1
5 Triple Data Encryption Algorithm (TDEA)	1
5.1 Definition of the TDEA algorithm	1
5.2 Use of the TDEA algorithm	2
6 RSA encryption algorithm	2
6.1 Definition of the RSA algorithm.....	2
6.2 Use of the RSA algorithm.....	2
7 AES encryption algorithm.....	2
7.1 Definition of the AES algorithm	2
7.2 Use of the AES algorithm	2
8 SM4 encryption algorithm.....	2
8.1 Definition of the SM4 algorithm	2
8.2 Use of the SM4 algorithm	2
9 ECIES algorithm.....	3
9.1 Definition of the ECIES algorithm	3
9.2 Use of the ECIES algorithm	3
Annex A (informative) Using key encapsulation mechanisms for establishment of PIN encryption keys.....	4
A.1 Overview	4
A.2 Acceptable key encapsulation mechanisms.....	4
A.3 Acceptable PIN block formats	4
A.4 Replay protection	5
A.5 Origin authentication	5
A.6 Public key authenticity and integrity	5
A.7 Key Usage.....	5
A.8 Example PIN change mechanism using RSA.....	6
A.9 Example mechanism using Elliptic Curve Cryptography	10