SLS 1057 : 1995
(ISO 9564-1: 1991)

Sri Lanka Standard

# BANKING - PERSONAL IDENTIFICATION NUMBER MANAGEMENT AND SECURITY - PARt 1 : PIN PROTECTION PRINCIPLES AND TECHNIQUES

Gr. L

SRI LANKA STANDARDS INSTITUTION

SLS 1057 : 1995
ISO 9564 -1 : 1991

# Sri Lanka Standard
# BANKING PERSONAL IDENTIFICATION NUMBER MANAGEMENT AND SECURITY - PART 1 : PIN PROTECTION PRINCIPLES AND TECHNEQUES

## NATIONAL FOREWORD

This standard was finalized by th Sectoral Committee on Information Technology and was authorized for adoption and publication as a Sri Lanka Standard by the Council of the Sri Lanka Standards Institution on 1995-05-25.

This Sri Lanka Standard is identical with ISO 9564 - 1 : 1991 Banking - Personal Identification Number Management and Security - Part 1 : PIN protection principles and techneques, published by the International Organization for Standardization (ISO).

## Terminology and conventions

The text of the International standard has been accepted as suitable for publication, without deviation, as a Sri Lanka Standard. However, certain terminology and conventions are not identical with those used in Sri Lanka Standards, attention is therefore drawn to the following:

a) Wherever the words 'International Standard/publication' appear, referring to this standard they should be interpreted as "Sri Lanka Standard".

Wherever page numbers are quoted, they are ISO page numbers.

CROSS - REFERENCES

| International Standard | Corresponding Sri Lanka Standards |
|---|---|
| ISO 7812-1 : 1993, Identification cards, Identification of issuers - Part 1 : Numbering system. | SLS 1033 : Part 1 : 1994 - Identification cards -Identification of issuers Part 1 : Numbering System. |
| ISO 7812 - 2 : 1993,Identification - Identification of issuers - Part 2 : Application and registration procedures | SLS 1033 : Part 2 : 1994 - Identification cards Identification of issuers Part 2 : Application procedures |
| ISO 8583 : 1987, Bank card originated messages - Interchange message specifications -Content for financial transactions | SLS * , Bank card originated messages Interchange message specifications- Content for financial transactions |
| ISO 8908 : 1991,Banking and related financial services - - Vocabulary and data elements. | SLS * ,Banking and related financial services - Vocabulary and data elements. |
| ISO 9807 : 1991, Banking and related financial services - Requirements for message authentication (retail). | SLS 1047 : 1995 Banking and related financial services - Requirements for message authentication (retail) |

* Under preperation

-/ltf.

# INTERNATIONAL STANDARD

# ISO 9564-1

First edition
1991-12-15

## Banking — Personal Identification Number management and security —

## Part 1:
PIN protection principles and techniques

*Banque — Gestion et sécurité du numéro personnel d'identification —*
*Partie 1: Principes et techniques de protection du PIN*

Reference number
ISO 9564-1:1991(E)

## Contents


Page

1 Scope ..... 1

2 Normative references ..... 1

3 Definitions ..... 2

4 Basic principles of PIN management ..... 3

5 PIN pads ..... 4

5.1 Character set ..... 4

5.2 Character representation ..... 4

5.3 PIN entry ..... 4

5.4 Packaging considerations ..... 4

6 PIN security issues ..... 5

6.1 PIN control procedures ..... 5

6.2 PIN encipherment ..... 5

6.3 Physical security ..... 6

7 Techniques for management/protection of account-related PIN functions ..... 7

7.1 PIN length ..... 7

7.2 PIN selection ..... 7

7.3 PIN delivery and issuance ..... 8

7.4 PIN change ..... 9

7.5 Disposal of waste material and returned PIN mailers ..... 9

7.6 PIN activation ..... 10

7.7 PIN storage ..... 10

7.8 PIN deactivation ..... 10

8 Techniques for management/protection of transaction-related PIN functions ..... 10

8.1 PIN entry ..... 10


© ISO 1991
All rights reserved. No part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from the publisher.

International Organization for Standardization
Case Postale 56 • CH-1211 Genève 20 • Switzerland

Printed in Switzerland

8.2 Protection of PIN during transmission ..... 10

8.3 Standard PIN block formats ..... 11

8.4 Other PIN block formats ..... 12

8.5 PIN verification ..... 12

8.6 Journaling of transactions containing PIN data ..... 12

9 Approval procedure for encipherment algorithms ..... 13

**Annexes**

A Procedure for approval of an encipherment algorithm ..... 14

B General principles of key management ..... 16

C PIN verification techniques ..... 18

D PIN entry device ..... 19

E Example of pseudo-random PIN generation ..... 21

F Additional guidelines for PIN pad design ..... 22

G Guidance on clearing and destruction procedures for sensitive data ..... 25

H Information for customers ..... 28