

13

SLS 1053 : 1995
(ISO 8730 : 1990)

Sri Lanka Standard

**BANKING - REQUIREMENTS FOR MESSAGE AUTHENTICATION
(WHOLESALE)**

Gr. M

SRI LANKA STANDARDS INSTITUTION

SLS 1053 : 1995
ISO 8730 : 1990

Sri Lanka Standard
BANKING - REQUIREMENTS FOR MESSAGES AUTHENTICATION
(WHOLESALE)

NATIONAL FOREWORD

This standard was finalized by the 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 8730 : 1990 Banking -Requirements for message authentication (wholesale), 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 Standards

ISO 7746 : 1988, Banking -
Telex formats for interbank
payment messages

ISO 7982 - 1 1987, Bank
telecommunication- Fund
transfer messages- Part 1,
Vocabulary and data

ISO 8731- 1 1987, Banking -
-Approved algorithms for
message authentication -
-Part 1 : DEA

ISO 8732 : 1988, Banking - Key
management (wholesale)

ISO 10126-1 : 1991, Banking -
Procedures for message
encipherment (wholesale)-
Part 1 : General principles

ISO 10126-2 : 1991, Banking -
Procedures for message
encipherment (wholesale)-
Part 2 : Algorithm

Corresponding Sri Lanka Standards

SLS 1051 : 1995 Banking - Telex
formats for interbank payment
messages

SLS 1045 : 1995 Bank telecommuni-
-cation - Fund, transfer messages -
Part 1 : Vocabulary and data

SLS 1054 : 1995, Banking - Approved
algorithms for message authenti-
-cation - Part 1 : DEA

SLS 1055 : 1995, Banking - Key
management (wholesale)

SLS 1058 : Part 1 : 1995, Banking
- Procedures for message
encipherment (wholesale) - Part 1
: General principles

SLS 1058 : Part 2 : 1995, Banking
-Procedures for message encipher-
-ment (wholesale) - Part 2
Algorithm

-/ltf.

INTERNATIONAL STANDARD

**ISO
8730**

Second edition
1990-05-15

Banking — Requirements for message authentication (wholesale)

Opérations bancaires — Spécifications liées à l'authentification des messages



Reference number
ISO 8730 : 1990 (E)

Contents

	Page
Foreword	iii
Introduction	v
1 Scope	1
2 Normative references	1
3 Definitions	1
4 Protection	3
5 Generation and checking of the Message Authentication Code (MAC)	3
6 Procedures for message authentication	3
7 Approval procedure for authentication algorithms	6
Annexes	
A Procedure for review of alternative authentication algorithms	7
B Risks associated with communications control characters	9
C Protection against duplication and loss	11
D Example of message authentication for coded character sets: DEA	12
E Example of message authentication for coded character sets: MAA	18
F Framework for message authentication of standard telex formats	23
G A pseudo-random key generator	25

© ISO 1990

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