

SLS 1047 : 1995  
(ISO 9807 : 1991)

Sri Lanka Standard

**BANKING AND RELATED FINANCIAL SERVICES - REQUIREMENTS  
FOR MESSAGE AUTHENTICATION (RETAIL)**

Gr. F

SRI LANKA STANDARDS INSTITUTION

SLS 1047 : 1995  
ISO 9807 : 1991

**Sri Lanka Standard**  
**BANKING AND RELATED FINANCIAL SERVICES - REQUIREMENTS**  
**FOR MESSAGE AUTHENTICATION (RETAIL)**

**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 9807:1991 Banking and related financial services - Requirements for message authentication (retail), 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 8730:1990, Banking - Requirements for message authentication (wholesale).

SLS 1053 : 1995 Banking- Requirements for message authentication (wholesale).

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

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

ISO 7812-2:1987, Banking - Approved algorithms for message authentication-Part : Message authenticator algorithms.

SLS 1054 : Part 2 : 1995,-Banking -Approved algorithms for message authentication Part 2 : Message authenticatore algorithms.

-/lrf.

# INTERNATIONAL STANDARD

**ISO**  
**9807**

First edition  
1991-12-15

---

---

## **Banking and related financial services — Requirements for message authentication (retail)**

*Banque et services financiers liés aux opérations bancaires —  
Spécifications liées à l'authentification des messages (service aux  
particuliers)*



Reference number  
ISO 9807:1991(E)

## Contents

	Page
1 Scope .....	1
2 Normative references .....	1
3 Definitions .....	1
4 Procedures for message authentication .....	2
4.1 Authentication keys .....	2
4.2 Authentication elements .....	2
4.3 MAC length .....	2
4.4 MAC generation .....	2
4.5 Placement of MAC .....	2
5 Verification of the MAC .....	2
6 Approval procedure for authentication algorithms .....	2

## Annexes

A Algorithms approved for calculation of MAC for authentication of retail messages .....	4
B Procedure for the review of alternative authentication algorithms .....	5
C Procedure to prevent exhaustive key determination .....	7
D Guidance on the selection of authentication elements .....	8
E Protection against duplication and loss .....	9
F Pseudo-random key generator .....	10
G Bibliography .....	11

© 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