

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