
**Banking — Requirements for message
authentication using symmetric
techniques**

*Banque — Exigences pour authentification des messages utilisant des
techniques symétriques*



PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

This document is a preview generated by EVS

© ISO 2004

All rights reserved. Unless otherwise specified, 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 either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	2
4 Protection	4
4.1 Protection of authentication keys	4
4.2 Authentication elements	5
4.3 Detection of duplication or loss	5
5 Procedures for message authentication	6
5.1 Preliminaries	6
5.2 Message format	6
5.3 Key generation	6
5.4 MAC Generation	7
5.5 MAC placement	7
5.6 MAC checking	7
6 Approved MAC algorithms	7
6.1 Overview of ISO/IEC 9797-1	7
6.2 Overview of ISO/IEC 9797-2	9
6.3 Implementation recommendations	9
Annex A (normative) Approved block ciphers for message authentication	11
Annex B (informative) Message authentication for coded character sets	13
Annex C (informative) Examples of message authentication for coded characters sets	18
Annex D (informative) Framework for message authentication of standard telex formats	23
Annex E (informative) Protection against duplication and loss using MIDs	25
Annex F (informative) Deterministic (pseudo-random) bit generator	26
Annex G (informative) Session key derivation	27
Annex H (informative) General tutorial information	28
Bibliography	29

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO 16609 was prepared by Technical Committee ISO/TC 68, *Banking, securities and other financial services*, Subcommittee SC 6, *Retail financial services*.

This first edition of ISO 16609 cancels and replaces ISO 8730:1990, ISO 8731-1:1987, ISO 8731-2:1992 and ISO 9807:1991, of which it constitutes a technical revision.

Introduction

A MAC (message authentication code) is a data field used to verify the authenticity of a message, generated by the sender of the message and transmitted together with it. The MAC enables an intended recipient to detect if the message has been altered and, if so, whether such an alteration arises by accident or with intent to defraud.

This International Standard has been prepared so that institutions involved in banking activities wishing to implement message authentication can do so in a secure manner and in a way that facilitates interoperability between separate implementations.

The requirements of this International Standard are compatible with those in the editions of ISO 8730 and ISO 9807 it replaces.

This document is a preview generated by EVS

Banking — Requirements for message authentication using symmetric techniques

1 Scope

This International Standard specifies procedures, independent of the transmission process, for protecting the integrity of transmitted banking messages and for verifying that a message has originated from an authorized source. It also specifies a method by which block ciphers can be approved for use in the authentication of banking messages. In addition, because of the necessity for both members in a communicating pair to use the same means for data representation, it defines some methods for data representation. A list of block ciphers approved for the calculation of a message authentication code (MAC), as well as the method to be used to approve additional block ciphers, is also provided. The authentication methods it defines are applicable to messages formatted and transmitted both as coded character sets and as binary data.

This International Standard is designed for use with symmetric algorithms where both sender and receiver use the same key. It does not specify methods for establishing the shared key, nor does it provide for encipherment for the protection of messages against unauthorized disclosure. Its application will not protect the user against internal fraud by sender or receiver, or forgery of a MAC by the receiver.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 7746:1998, *Banking — Telex formats for inter-bank messages*

ISO 8583:1993, *Financial transaction card originated messages — Interchange message specifications*

ISO 8601:2000, *Data elements and interchange formats — Information interchange — Representation of dates and times*

ISO 8732:1988, *Banking — Key management (wholesale)*

ISO/IEC 9797-1:1999, *Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher*

ISO/IEC 9797-2:2002, *Information technology — Security techniques — Message Authentication Codes (MACs) — Part 2: Mechanisms using a hash-function*

ISO/IEC 10116:1997, *Information technology — Security techniques — Modes of operation for an n-bit block cipher*

ISO/IEC 10118-3:1998, *Information technology — Security techniques — Hash-functions — Part 3: Dedicated hash-functions*

ISO 11568-1:1994, *Banking — Key management (retail) — Part 1: Introduction to key management*

ISO 11568-2:1994, *Banking — Key management (retail) — Part 2: Key management techniques for symmetric ciphers*

ISO 11568-3:1994, *Banking — Key management (retail) — Part 3: Key life cycle for symmetric ciphers*

ISO 13491 (all parts) *Banking — Secure cryptographic devices (retail)*

ANSI X3.92:1981, *American National Standard for Information Systems — Data encryption algorithm*

ANSI X9.52:1998, *American National Standard for Financial Services — Triple data encryption algorithm, modes of operation*

3 Terms and definitions

For the purposes of this document the following terms and definitions apply.

**3.1
algorithm**
specified mathematical process for computation or set of rules which, if followed, will give a prescribed result

**3.2
authentication**
process used between a sender and a receiver to ensure data integrity and provide data origin authentication

**3.3
authentication algorithm**
algorithm used, together with an authentication key and one or more authentication elements, for authentication

**3.4
authentication element**
message element that is to be protected by authentication

**3.5
authentication key**
cryptographic key used for authentication

**3.6
beneficiary [party]**
ultimate party (can be more than one) to be credited or paid as a result of a transfer

**3.7
block cipher**
algorithm for computing a function which maps a fixed length string of bits and a secret key to another string of bits with the same fixed length

**3.8
bias**
condition where, during the generation of random or pseudo-random numbers, the occurrence of some numbers is more likely than others

**3.9
cryptoperiod**
defined period of time during which a specific cryptographic key is authorized for use, or during which time the cryptographic keys in a given system may remain in effect