INTERNATIONAL STANDARD

ISO 16609

Second edition
2012-03-15

Financial services — Requirements for message authentication using symmetric techniques

Services financiers — Exigences pour l'authentification des messages utilisant des techniques symétriques

Reference number
ISO 16609:2012(E)

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

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, *Financial services*, Subcommittee SC 2, *Financial services, security*.

This second edition cancels and replaces the first edition (ISO 16609:2004), which has been technically revised.

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 whether the message has been altered. While non-keyed message integrity methods, e.g. checksums, only protect against accidental alteration of the message, MACs additionally protect against deliberate alteration since the adversary would not have access to the key used to generate the MAC.

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

This International Standard identifies ciphers, hash functions and algorithms from ISO 9797 (all parts) that are specifically approved for secure banking purposes.

Financial services — 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. A list of block ciphers approved for the calculation of a message authentication code (MAC) 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 perpetrated by the sender or the receiver, nor against 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/IEC 9797-1:2011, *Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher*

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

ISO 11568-1, *Banking — Key management (retail) — Part 1: Principles*

ISO 11568-2, *Financial services — Key management (retail) — Part 2: Symmetric ciphers, their key management and life cycle*

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