American National Standard

INCITS/ISO/IEC 9797-2:2011[2012]

(ISO/IEC 9797-2:2011, IDT)

Reaffirmed as
INCITS/ISO/IEC 9797-2:2011 (R2017)

Information technology - Security techniques - Message Authentication Codes (MACs) - Part 2: Mechanisms using a dedicated hash-function

Developed by

incits SM

Where IT all begins

Approved American National Standard

ANSI

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.

Adopted by INCITS (InterNational Committee for Information Technology Standards) as an American National Standard.

Date of ANSI Approval: 8/21/12

Published by American National Standards Institute,
25 West 43rd Street, New York, New York 10036

Second edition
2011-05-01

Corrected version
2011-06-15

Information technology — Security techniques — Message Authentication Codes (MACs) —

Part 2: Mechanisms using a dedicated hash-function

Technologies de l'information — Techniques de sécurité — Codes d'authentification de message (MAC) —

Partie 2: Mécanismes utilisant une fonction de hachage dédiée

Reference number
ISO/IEC 9797-2:2011(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

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

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

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

ISO/IEC 9797-2 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

This second edition cancels and replaces the first edition (ISO/IEC 9797-2:2002), which has been technically revised by including MAC algorithms based on Dedicated Hash-Functions 4 – 7 of ISO/IEC 10118-3:2004 and Dedicated Hash-Function 8 of ISO/IEC 10118-3/Amd.1:2006.

ISO/IEC 9797 consists of the following parts, under the general title *Information technology — Security techniques — Message Authentication Codes (MACs)*:

— Part 1: Mechanisms using a block cipher

— Part 2: Mechanisms using a dedicated hash-function

— Part 3: Mechanisms using a universal hash-function

Further parts may follow.

This corrected version of ISO/IEC 9797-2:2011 incorporates corrections to subclauses 3.14, 6.3, 6.3.5 and 6.3.6.

Introduction

The International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) draw attention to the fact that it is claimed that compliance with this document may involve the use of a patent concerning MAC Algorithm 1 (MDx-MAC) given in Clause 6.

ISO and IEC take no position concerning the evidence, validity and scope of this patent right.

The holder of this patent right has assured ISO and IEC that he is willing to negotiate licenses under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statement of the holder of this patent right is registered with ISO and IEC. Information may be obtained from:

Entrust Technologies, Technology Licensing Dept., 1000 Innovation Drive, Ottawa, Ontario, Canada K2K 3E7.

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