

---

---

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

**Part 3:  
Mechanisms using a universal hash-  
function**

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

*Partie 3: Mécanismes utilisant une fonction de hachage universelle*



**COPYRIGHT PROTECTED DOCUMENT**

© ISO/IEC 2011

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](mailto:copyright@iso.org)  
Web [www.iso.org](http://www.iso.org)

Published in Switzerland

# Contents

Page

Foreword .....	iv
Introduction.....	v
1 Scope .....	1
2 Normative references .....	1
3 Terms and definitions .....	1
4 Symbols and abbreviated terms .....	2
5 General model.....	4
6 Mechanisms .....	5
6.1 Introduction.....	5
6.2 UMAC .....	5
6.2.1 Description of UMAC.....	5
6.2.2 Requirements.....	5
6.2.3 Notation and auxiliary functions.....	5
6.2.4 Key preprocessing .....	9
6.2.5 Message preprocessing.....	9
6.2.6 Message hashing.....	9
6.2.7 Layered hash-functions .....	10
6.2.8 Finalization .....	12
6.3 Badger .....	12
6.3.1 Description of Badger.....	12
6.3.2 Requirements.....	12
6.3.3 Notation and auxiliary functions.....	13
6.3.4 Key preprocessing .....	13
6.3.5 Message preprocessing.....	14
6.3.6 Message hashing.....	14
6.3.7 Finalization .....	16
6.4 Poly1305-AES .....	16
6.4.1 Description of Poly1305-AES .....	16
6.4.2 Requirements.....	16
6.4.3 Key preprocessing .....	16
6.4.4 Message preprocessing.....	16
6.4.5 Message hashing.....	17
6.4.6 Finalization .....	17
6.5 GMAC .....	18
6.5.1 Description of GMAC .....	18
6.5.2 Requirements.....	18
6.5.3 Notation and auxiliary functions.....	18
6.5.4 Key preprocessing .....	19
6.5.5 Message preprocessing.....	19
6.5.6 Message hashing.....	19
6.5.7 Finalization .....	19
Annex A (normative) Object Identifiers .....	20
Annex B (informative) Test Vectors .....	22
Annex C (informative) Security Information.....	24
Bibliography.....	25

## 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.

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

ISO/IEC 9797-3 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

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*

## Introduction

In an IT environment, it is often required that one can verify that electronic data has not been altered in an unauthorized manner and that one can provide assurance that a message has been originated by an entity in possession of the secret key. A MAC (Message Authentication Code) algorithm is a commonly used data integrity mechanism that can satisfy these requirements.

This part of ISO/IEC 9797 specifies four MAC algorithms using universal hash-functions: UMAC, Badger, Poly1305-AES and GMAC.

These mechanisms can be used as data integrity mechanisms to verify that data has not been altered in an unauthorized manner. They can also be used as message authentication mechanisms to provide assurance that a message has been originated by an entity in possession of the secret key. The strength of the data integrity mechanism and message authentication mechanism is dependent on the length (in bits) and secrecy of the key, on the length (in bits) of a hash-code produced by the hash-function, on the strength of the hash-function, on the length (in bits) of the MAC, and on the specific mechanism.

NOTE A general framework for the provision of integrity services is specified in ISO/IEC 10181-6<sup>[7]</sup>.

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

## Part 3: Mechanisms using a universal hash-function

### 1 Scope

This part of ISO/IEC 9797 specifies the following MAC algorithms that use a secret key and a universal hash-function with an  $n$ -bit result to calculate an  $m$ -bit MAC based on the block ciphers specified in ISO/IEC 18033-3 and the stream ciphers specified in ISO/IEC 18033-4:

- a) UMAC;
- b) Badger;
- c) Poly1305-AES;
- d) GMAC.

### 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, *Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher*

ISO/IEC 18031, *Information technology — Security techniques — Random bit generation*

ISO/IEC 18033-3, *Information technology — Security techniques — Encryption algorithms — Part 3: Block ciphers*

ISO/IEC 18033-4, *Information technology — Security techniques — Encryption algorithms — Part 4: Stream ciphers*