

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)





**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
<b>1 Scope .....</b>	<b>1</b>
<b>2 Normative references .....</b>	<b>1</b>
<b>3 Terms and definitions .....</b>	<b>2</b>
<b>4 Symbols and notation .....</b>	<b>4</b>
<b>5 Requirements.....</b>	<b>5</b>
<b>6 MAC Algorithm 1 .....</b>	<b>6</b>
<b>6.1 Description of MAC Algorithm 1 .....</b>	<b>7</b>
<b>6.1.1 Step 1 (key expansion).....</b>	<b>7</b>
<b>6.1.2 Step 2 (modification of the constants and the IV).....</b>	<b>7</b>
<b>6.1.3 Step 3 (hashing operation) .....</b>	<b>7</b>
<b>6.1.4 Step 4 (output transformation).....</b>	<b>8</b>
<b>6.1.5 Step 5 (truncation).....</b>	<b>8</b>
<b>6.2 Efficiency.....</b>	<b>8</b>
<b>6.3 Computation of the constants.....</b>	<b>8</b>
<b>6.3.1 Dedicated Hash-Function 1 (RIPEMD-160) .....</b>	<b>9</b>
<b>6.3.2 Dedicated Hash-Function 2 (RIPEMD-128) .....</b>	<b>9</b>
<b>6.3.3 Dedicated Hash-Function 3 (SHA-1).....</b>	<b>10</b>
<b>6.3.4 Dedicated Hash-Function 4 (SHA-256).....</b>	<b>10</b>
<b>6.3.5 Dedicated Hash-Function 5 (SHA-512).....</b>	<b>10</b>
<b>6.3.6 Dedicated Hash-Function 6 (SHA-384).....</b>	<b>11</b>
<b>6.3.7 Dedicated Hash-Function 8 (SHA-224).....</b>	<b>11</b>
<b>7 MAC Algorithm 2 .....</b>	<b>12</b>
<b>7.1 Description of MAC Algorithm 2 .....</b>	<b>12</b>
<b>7.1.1 Step 1 (key expansion).....</b>	<b>12</b>
<b>7.1.2 Step 2 (hashing operation) .....</b>	<b>12</b>
<b>7.1.3 Step 3 (output transformation).....</b>	<b>12</b>
<b>7.1.4 Step 4 (truncation).....</b>	<b>13</b>
<b>7.2 Efficiency.....</b>	<b>13</b>
<b>8 MAC Algorithm 3 .....</b>	<b>13</b>
<b>8.1 Description of MAC Algorithm 3 .....</b>	<b>13</b>
<b>8.1.1 Step 1 (key expansion).....</b>	<b>13</b>
<b>8.1.2 Step 2 (modification of the constants and the IV).....</b>	<b>14</b>
<b>8.1.3 Step 3 (padding) .....</b>	<b>14</b>
<b>8.1.4 Step 4 (application of the round-function).....</b>	<b>14</b>
<b>8.1.5 Step 5 (truncation).....</b>	<b>15</b>
<b>8.2 Efficiency.....</b>	<b>15</b>
<b>Annex A (normative) ASN.1 Module .....</b>	<b>16</b>
<b>Annex B (informative) Examples .....</b>	<b>17</b>
<b>Annex C (informative) A security analysis of the MAC algorithms.....</b>	<b>37</b>
<b>Bibliography.....</b>	<b>39</b>