

---

---

**Financial services — Requirements  
for message authentication using  
symmetric techniques**

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





**COPYRIGHT PROTECTED DOCUMENT**

© ISO 2022

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office  
CP 401 • Ch. de Blandonnet 8  
CH-1214 Vernier, Geneva  
Phone: +41 22 749 01 11  
Email: [copyright@iso.org](mailto:copyright@iso.org)  
Website: [www.iso.org](http://www.iso.org)

Published in Switzerland

# Contents

Page

<b>Foreword</b> .....	<b>iv</b>
<b>Introduction</b> .....	<b>v</b>
<b>1 Scope</b> .....	<b>1</b>
<b>2 Normative references</b> .....	<b>1</b>
<b>3 Terms and definitions</b> .....	<b>1</b>
<b>4 Principles</b> .....	<b>3</b>
4.1 Protection of authentication keys.....	3
4.2 Message authentication elements.....	3
4.3 Detection of duplication, loss or sequence errors.....	4
<b>5 Procedures for message authentication</b> .....	<b>4</b>
5.1 MAC generation.....	4
5.2 MAC placement.....	5
5.3 MAC verification.....	5
5.4 Approved authentication mechanisms based on the ISO/IEC 9797 series.....	5
5.4.1 General.....	5
5.4.2 Approved message authentication mechanisms based on ISO/IEC 9797-1.....	5
5.4.3 Approved message authentication mechanisms based on ISO/IEC 9797-2.....	6
5.4.4 Approved message authentication mechanisms based on ISO/IEC 9797-3.....	7
5.4.5 Implementation recommendations.....	8
<b>Annex A (informative) Protection against duplication and loss using MIDs</b> .....	<b>9</b>
<b>Annex B (informative) General tutorial information</b> .....	<b>11</b>
<b>Bibliography</b> .....	<b>13</b>