

INTERNATIONAL
STANDARD

ISO/IEC
24759

Third edition
2017-03

**Information technology — Security
techniques — Test requirements for
cryptographic modules**

*Technologies de l'information — Techniques de sécurité — Exigences
d'essai pour modules cryptographiques*



Reference number
ISO/IEC 24759:2017(E)

© ISO/IEC 2017



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2017, Published in Switzerland

All rights reserved. Unless otherwise specified, 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
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

	Page
Foreword	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Symbols and abbreviated terms	1
5 Document organization	1
5.1 General	1
5.2 Assertions and security requirements	2
6 Security requirements	2
6.1 General	2
6.2 Cryptographic module specification	3
6.2.1 Cryptographic module specification general requirements	3
6.2.2 Types of cryptographic modules	3
6.2.3 Cryptographic boundary	5
6.2.4 Modes of operations	13
6.3 Cryptographic module interfaces	17
6.3.1 Cryptographic module interfaces general requirements	17
6.3.2 Types of interfaces	20
6.3.3 Definition of interfaces	20
6.3.4 Trusted channel	30
6.4 Roles, services, and authentication	32
6.4.1 Roles, services, and authentication general requirements	32
6.4.2 Roles	33
6.4.3 Services	34
6.4.4 Authentication	42
6.5 Software/Firmware security	49
6.6 Operational environment	57
6.6.1 Operational environment general requirements	57
6.6.2 Operating system requirements for limited or non-modifiable operational environments	57
6.6.3 Operating system requirements for modifiable operational environments	58
6.7 Physical security	68
6.7.1 Physical security embodiments	68
6.7.2 Physical security general requirements	69
6.7.3 Physical security requirements for each physical security embodiment	75
6.7.4 Environmental failure protection/testing	86
6.8 Non-invasive security	89
6.9 Sensitive security parameter management	91
6.9.1 Sensitive security parameter management general requirements	91
6.9.2 Random bit generators	92
6.9.3 Sensitive security parameter generation	93
6.9.4 Sensitive security parameter establishment	94
6.9.5 Sensitive security parameter entry and output	94
6.9.6 Sensitive security parameter storage	98
6.9.7 Sensitive security parameter zeroisation	99
6.10 Self-tests	102
6.10.1 Self-test general requirements	102
6.10.2 Pre-operational self-tests	105
6.10.3 Conditional self-tests	109
6.11 Life-cycle assurance	119
6.11.1 Life-cycle assurance general requirements	119
6.11.2 Configuration management	119