

INTERNATIONAL
STANDARD

ISO/IEC
19790

First edition
2006-03-01

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

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

Reference number
ISO/IEC 19790:2006(E)



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.

© ISO/IEC 2006

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
Web 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 Abbreviated terms	9
5 Cryptographic module security levels	9
5.1 Security Level 1.....	10
5.2 Security Level 2.....	10
5.3 Security Level 3.....	10
5.4 Security Level 4.....	11
6 Functional security objectives	11
7 Security requirements	12
7.1 Cryptographic module specification	14
7.2 Cryptographic module ports and interfaces.....	15
7.3 Roles, services, and authentication.....	16
7.4 Finite state model	18
7.5 Physical security.....	19
7.6 Operational environment	26
7.7 Cryptographic key management.....	29
7.8 Self-tests.....	31
7.9 Design assurance	34
7.10 Mitigation of other attacks	36
Annex A (normative) Documentation requirements.....	38
Annex B (normative) Cryptographic module security policy	42
Annex C (normative) Approved protection profiles	44
Annex D (informative) Approved security functions	45
Annex E (informative) Approved key establishment methods	47
Annex F (informative) Recommended software development practices.....	48
Annex G (informative) Examples of mitigation of other attacks	50
Bibliography	51