

---

---

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

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

**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.

This document is a preview generated by EVS

© 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](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 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

## 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 19790 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

## Introduction

In Information Technology there is an ever-increasing need to use cryptographic mechanisms such as the protection of data against unauthorised disclosure or manipulation, for entity authentication and for non-repudiation. The security and reliability of such mechanisms are directly dependent on the cryptographic modules in which they are implemented.

This International Standard provides for four increasing, qualitative levels of security requirements intended to cover a wide range of potential applications and environments. The security requirements cover areas relative to the design and implementation of a cryptographic module. These areas include cryptographic module specification; cryptographic module ports and interfaces; roles, services, and authentication; finite state model; physical security; operational environment; cryptographic key management; self-tests; design assurance; and mitigation of other attacks.

The overall security level of a cryptographic module must be chosen to provide a level of security appropriate for the security requirements of the application and environment in which the module is to be utilized and for the security services that the module is to provide. The responsible authority in each organization should ensure that their computer and telecommunication systems that utilize cryptographic modules provide an acceptable level of security for the given application and environment. Since each authority is responsible for selecting which approved security functions are appropriate for a given application, compliance with this International Standard does not imply either full interoperability or mutual acceptance of compliant products. The importance of security awareness and of making information security a management priority should be communicated to all concerned.

Information security requirements vary for different applications; organizations should identify their information resources and determine the sensitivity to and the potential impact of a loss by implementing appropriate controls. Controls include, but are not limited to

- physical and environmental controls;
- software development;
- backup and contingency plans; and
- information and data controls.

These controls are only as effective as the administration of appropriate security policies and procedures within the operational environment.

This International Standard will be revised later, if a new work item is approved, in order to improve the links with Common Criteria scheme (ISO/IEC 15408).

This International Standard is derived from NIST Federal Information Processing Standard (FIPS) PUB 140-2 (see Bibliography [1]).

This document is a preview generated by EVS

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

## 1 Scope

This International Standard specifies the security requirements for a cryptographic module utilized within a security system protecting sensitive information in computer and telecommunication systems. This International Standard defines four security levels for cryptographic modules to provide for a wide spectrum of data sensitivity (e.g., low value administrative data, million dollar funds transfers, and life protecting data) and a diversity of application environments (e.g., a guarded facility, an office, and a completely unprotected location). Four security levels are specified for each of 10 requirement areas. Each security level offers an increase in security over the preceding level.

While the security requirements specified in this International Standard are intended to maintain the security provided by a cryptographic module, compliance to this International Standard is not sufficient to ensure that a particular module is secure or that the security provided by the module is sufficient and acceptable to the owner of the information that is being protected.

## 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 15408 (all parts), *Information technology — Security techniques — Evaluation criteria for IT security*

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

## 3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

### 3.1

#### **approval authority**

any national or international organisation/authority mandated to approve and/or evaluate security functions

### 3.2

#### **approved**

ISO/IEC approved or approval authority approved

### 3.3

#### **approved mode of operation**

mode of the cryptographic module that employs only approved security functions

**NOTE** Not to be confused with a specific mode of an approved security function, e.g., Cipher Block Chaining (CBC) mode.