

This is a preview of "INCITS/ISO/IEC 24759...". Click here to purchase the full version from the ANSI store.

(ISO/IEC 24759:2014,
Corrected 2015-12-15, IDT)

American National Standard

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

Developed by



Where IT all begins



This is a preview of "INCITS/ISO/IEC 24759...". [Click here to purchase the full version from the ANSI store.](#)

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.

Adopted by INCITS (InterNational Committee for Information Technology Standards) as an American National Standard.

Date of ANSI Approval: 12/17/2014

Published by American National Standards Institute,
25 West 43rd Street, New York, New York 10036

Copyright 2014 by Information Technology Industry Council
(ITI). All rights reserved.

These materials are subject to copyright claims of International Standardization Organization (ISO), International Electrotechnical Commission (IEC), American National Standards Institute (ANSI), and Information Technology Industry Council (ITI). Not for resale. No part of this publication may be reproduced in any form, including an electronic retrieval system, without the prior written permission of ITI. All requests pertaining to this standard should be submitted to ITI, 1101 K Street NW, Suite 610, Washington DC 20005.

Printed in the United States of America

This is a preview of "INCITS/ISO/IEC 24759...". [Click here to purchase the full version from the ANSI store.](#)

Second edition
2014-02-01

Corrected version
2015-12-15

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 24759:2014(E)



© ISO/IEC 2014



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2014, 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

This is a preview of "INCITS/ISO/IEC 24759...". Click here to purchase the full version from the ANSI store.

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	1
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.....	29
6.4 Roles, services, and authentication	31
6.4.1 Roles, services, and authentication general requirements	31
6.4.2 Roles	32
6.4.3 Services	33
6.4.4 Authentication	41
6.5 Software/Firmware security.....	49
6.6 Operational environment	56
6.6.1 Operational environment general requirements	56
6.6.2 Operating system requirements for limited or non-modifiable operational environments	57
6.6.3 Operating system requirements for modifiable operational environments	57
6.7 Physical security	67
6.7.1 Physical security embodiments.....	67
6.7.2 Physical security general requirements	68
6.7.3 Physical security requirements for each physical security embodiment	74
6.7.4 Environmental failure protection/testing	85
6.8 Non-invasive security	88
6.9 Sensitive security parameter management	90
6.9.1 Sensitive security parameter management general requirements	90
6.9.2 Random bit generators	92
6.9.3 Sensitive security parameter generation	92
6.9.4 Sensitive security parameter establishment	93
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	98
6.10 Self-tests.....	101
6.10.1 Self-test general requirements.....	101
6.10.2 Pre-operational self-tests	105
6.10.3 Conditional self-tests	108
6.11 Life-cycle assurance	118
6.11.1 Life-cycle assurance general requirements	118
6.11.2 Configuration management.....	119
6.11.3 Design.....	120

This is a preview of "INCITS/ISO/IEC 24759...". [Click here to purchase the full version from the ANSI store.](#)

6.11.4	Finite state model	120
6.11.5	Development	124
6.11.6	Vendor testing	129
6.11.7	Delivery and operation	129
6.11.8	End of life.....	130
6.11.9	Guidance documents	131
6.12	Mitigation of other attacks	132
6.A	Documentation requirements.....	133
6.B	Cryptographic module security policy	133
6.C	Approved security functions	134
6.D	Approved sensitive security parameter generation and establishment methods	134
6.E	Approved authentication mechanisms	134
6.F	Approved non-invasive attack mitigation test metrics	135

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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: [Foreword - Supplementary information](#)

Technical Corrigendum 1 to ISO/IEC 24759:2014 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Security techniques*.

This corrected version of Technical corrigendum 1 to ISO/IEC 24759:2014 cancels and replaces the first edition (ISO/IEC 24759:2014/Cor 1:2015), incorporating the same technical revisions and miscellaneous editorial corrections showing in **red** text instead of black underlining:

- 6.2.3.2: AS02.15, AS02.16, AS02.17 and AS02.18 modified
- 6.3.3: AS03.04, AS03.07, AS03.10 and AS03.15 modified
- 6.3.4: AS03.19 modified
- 6.4.1: AS04.02 modified
- 6.4.2: AS04.05, AS04.06 and AS04.07 modified
- 6.4.3.1: AS04.11, AS04.13 and AS04.14
- 6.4.3.2 and AS04.20
- 6.4.4: AS04.39, AS04.40 and AS04.42 modified
- 6.5: AS05.05, AS05.06, AS05.07, AS05.08, AS05.13, AS05.17 and AS05.18 modified
- 6.8: AS08.04 modified
- 6.10.1: AS10.17 modified