This is a preview of "ISO/IEC 24759:2017". Click here to purchase the full version from the ANSI store.

INTERNATIONAL ISO/IEC

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

This is a preview of "ISO/IEC 24759:2017". Click here to purchase the full version from the ANSI store.

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

 © ISO/IEC 2017 – All rights reserved

This is a preview of "ISO/IEC 24759:2017". 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 ... 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

© ISO/IEC 2017 – All rights reserved

This is a preview of "ISO/IEC 24759:2017". Click here to purchase the full version from the ANSI store.

6.11.3 Design 121
6.11.4 Finite state model 121
6.11.5 Development 125
6.11.6 Vendor testing 129
6.11.7 Delivery and operation 130
6.11.8 End of life 131
6.11.9 Guidance documents 132
6.12 Mitigation of other attacks 133
6.13 Documentation requirements 134
6.14 Cryptographic module security policy 134
6.15 Approved security functions 135
6.16 Approved sensitive security parameter generation and establishment methods 135
6.17 Approved authentication mechanisms 135
6.18 Approved non-invasive attack mitigation test metrics 135

 © ISO/IEC 2017 – All rights reserved

This is a preview of "ISO/IEC 24759:2017". Click here to purchase the full version from the ANSI store.

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 ISO documents 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 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 voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

This document was prepared by ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

This third edition cancels and replaces the second edition (ISO/IEC 24759:2014), of which it constitutes a minor revision. It also incorporates the Technical Corrigendum ISO/IEC 24759:2014/Cor.1:2015.

The main changes compared to the previous edition (plus other minor editorial modifications) are as follows:

— References to ISO/IEC 19790:2012 have been corrected throughout:

— 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.

© ISO/IEC 2017 – All rights reserved

This is a preview of "ISO/IEC 24759:2017". Click here to purchase the full version from the ANSI store.

 © ISO/IEC 2017 – All rights reserved