TECHNICAL SPECIFICATION

ISO/IEC TS 20540

First edition
2018-05

Information technology — Security techniques — Testing cryptographic modules in their operational environment

Technologies de l'information — Techniques de sécurité — Test de modules cryptographiques dans leur environnement d'exploitation

iTeh Standards
(https://standards.iteh.ai)
Document Preview

ISO/IEC TS 20540:2018
https://standards.iteh.ai/catalog/standards/iso/690ae3f6-0ab1-4ed1-bc25-0af711fd303f/iso-iec-ts-20540-2018

Reference number
ISO/IEC TS 20540:2018(E)

© ISO/IEC 2018

iTeh Standards
(https://standards.iteh.ai)
Document Preview

ISO/IEC TS 20540:2018
https://standards.iteh.ai/catalog/standards/iso/690ae3f6-0ab1-4ed1-bc25-0af711fd303f/iso-iec-ts-20540-2018

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2018

All rights reserved. Unless otherwise specified, or required in the context of its implementation, 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
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

© ISO/IEC 2018 – All rights reserved

Contents

Page

Foreword ..... **v**
Introduction ..... **vi**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **2**
4 Abbreviated terms **5**
5 Document organization **5**
6 Context of operational testing **6**
7 Cryptographic modules **7**
7.1 General 7
7.2 Types of cryptographic modules 7
7.2.1 General 7
7.2.2 Software module 8
7.2.3 Firmware module 8
7.2.4 Hardware module 8
7.2.5 Hybrid software module 8
7.2.6 Hybrid firmware module 8
7.3 Cryptographic module application environments 8
7.4 Security products with cryptographic modules 9
7.5 Security requirements for cryptographic modules 10
7.5.1 General 10
7.5.2 Security Level 1 10
7.5.3 Security Level 2 11
7.5.4 Security Level 3 11
7.5.5 Security Level 4 12
7.6 Life-cycle assurance of cryptographic modules 12
7.7 Cryptographic module security policy 12
7.7.1 General 12
7.7.2 Cryptographic module specification 13
7.7.3 Cryptographic module interfaces 13
7.7.4 Roles, services, and authentication 13
7.7.5 Software/firmware security 13
7.7.6 Operational environment 14
7.7.7 Physical security 14
7.7.8 Non-invasive security 14
7.7.9 Sensitive security parameters management 14
7.7.10 Self-tests 14
7.7.11 Life-cycle assurance 15
7.7.12 Mitigation of other attacks 15
7.8 Intended purpose of validated cryptographic modules 15
8 The application environment **16**
8.1 Organizational security 16
8.2 Architecture of the application environment 16
9 The operational environment **17**
9.1 Security requirements related to cryptographic modules for their operational environment 17
9.1.1 General 17
9.1.2 Entropy sources 17
9.1.3 Audit mechanism 17
9.1.4 Physically unclonable function 17
9.2 Security assumptions for the operational environment 17

iTeh Standards
(https://standards.iteh.ai)
Document Preview
https://standards.iteh.ai/catalog/standards/iso/8f9ba1c0-c9b1-4ed1-bc25-0af711fd303f/iso-iec-ts-20540-2018

© ISO/IEC 2018 – All rights reserved

9.2.1 General 17
9.2.2 Security Level 1 18
9.2.3 Security Level 2 18
9.2.4 Security Level 3 19
9.2.5 Security Level 4 20

10 How to select cryptographic modules 21
10.1 General 21
10.2 Use policy 21
10.3 Cryptographic module assurance 23
10.4 Interoperability 23
10.5 Selection of security rating for SSP protection 23

11 Principles for operational testing 23
11.1 General 23
11.2 Assumptions 24
11.3 Operational testing activities 24
11.4 Competence for operational testers 25
11.5 Use of validated evidence 25
11.6 Documentation 25
11.7 Operational testing procedure 26

12 Recommendations for operational testing 26
12.1 General 26
12.2 Recommendations for assessing the installation, configuration, and operation of the cryptographic module 26
12.2.1 General 26
12.2.2 Assessing installation of the cryptographic module 27
12.2.3 Assessing the configuration of the cryptographic module 27
12.2.4 Assessing the correct operation of the cryptographic module 29
12.3 Recommendations for inspecting a key management system 29
12.4 Recommendations for inspecting the security requirements of authentication credentials 30
12.5 Recommendations for assessing the availability of cryptographic modules 31
12.6 Recommendations for identifying potential residual vulnerabilities of cryptographic modules 31
12.7 Checking for the organization's security policies 32

13 Reporting the results of operational testing 33

Annex A (informative) **Examples of validated cryptographic modules lists 34**

Annex B (informative) **Checklist for operational testing of cryptographic modules 35**

Bibliography 39

iTeh Standards
(https://standards.iteh.ai)
Document Preview
ISO/IEC TS 20540:2018
https://standards.iteh.ai/catalog/standards/iso/e30ae316-0ab1-4ed1-bc25-0af7111d303f/iso-iec-ts-20540-2018

 © ISO/IEC 2018 – All rights reserved

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 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 Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

iTeh Standards
(https://standards.iteh.ai)
Document Preview
ISO/IEC TS 20540:2018
https://standards.iteh.ai/catalog/standards/iso/690ae3f6-0ab1-4ed1-bc25-0af711fd303f/iso-iec-ts-20540-2018

© ISO/IEC 2018 – All rights reserved

Introduction

In information technology, there is an ever-increasing need to use cryptographic mechanisms such as the protection of data against unauthorized 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. Cryptographic modules are utilized within a security system to protect sensitive information in their application environment.

The purpose of this document is to describe the recommendations and checklists which help in the selection of cryptographic modules for deployment in a diversity of application environments. This document is helpful for a user and operational tester to verify correct deployment in the application environment.

Operational tests are performed to determine the suitability and proper usage of a cryptographic module in its application environment.

Cryptographic modules and their application environments are generally complex. When cryptographic modules are deployed in an operational environment, a minor error or mistake can affect the security of the whole operational and application environment. It is important to perform operational tests to ensure the proper usage of a cryptographic module in their operational environment. This document identifies the operational tests by providing:

— recommendations to perform a secure assessment of the cryptographic module installation, configuration and operation;

— recommendations for inspecting the key management system, protection of authentication credentials, and public and critical security parameters in the operational environment;

— recommendations for identifying cryptographic module vulnerabilities;

— checklists for the cryptographic algorithm policy, security guidance and regulation, security manage requirements, security level for each of the 11 requirement areas, the strength of the security function, etc.; and

— inspection recommendations to determine that the cryptographic module's deployment satisfies the security requirements.

iTeh Standards
(https://standards.iteh.ai)
Document Preview
ISO/IEC TS 20540:2018
https://standards.iteh.ai/catalog/standards/iec/60...-20540-2018

When the operational testing is performed by using this document, access to the text of ISO/IEC 19790 and ISO/IEC 24759 can be required.

© ISO/IEC 2018 – All rights reserved