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

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

COPYRIGHT PROTECTED DOCUMENT

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

Contents

Page

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*.

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.

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.

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

1 Scope

This document provides recommendations and checklists which can be used to support the specification and operational testing of cryptographic modules in their operational environment within an organization's security system.

The cryptographic modules have four security levels which ISO/IEC 19790 defines to provide for a wide spectrum of data sensitivity (e.g. low-value administrative data, million-dollar funds transfers, life-protecting data, personal identity information, and sensitive information used by government) and a diversity of application environments (e.g. a guarded facility, an office, removable media, and a completely unprotected location).

This document includes:

a) recommendations to perform secure assessing for cryptographic module installation, configuration and operation;

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

c) recommendations for identifying cryptographic module vulnerabilities;

d) 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

e) recommendations to determine that the cryptographic module's deployment satisfies the security requirements of the organization.

This document assumes that the cryptographic module has been validated as conformant with ISO/IEC 19790.

It can be used by an operational tester along with other recommendations if needed.

This document is limited to the security related to the cryptographic module. It does not include assessing the security of the operational or application environment. It does not define techniques for the identification, assessment and acceptance of the organization's operational risk.

The organization's accreditation, deployment and operation processes, shown in Figure 1, is not included to the scope of this document.

This document addresses operational testers who perform the operational testing for the cryptographic modules in their operational environment authorizing officials of cryptographic modules.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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 19790:2012, *Information technology — Security techniques — Security requirements for cryptographic modules*

ISO/IEC 24759, *Information technology — Security techniques — Test requirements for cryptographic modules*