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)

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*

## 3 Terms and definitions

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

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

**3.1**
**accreditation**
administrative process whereby authority is granted for the operation of the cryptographic module in its full operational environment including all of its non-IT parts

Note 1 to entry: The results of the *operational testing* (3.12) process may be an input to the accreditation process.

**3.2**
**administrator guidance**
written material that is used by the Crypto Officer and/or other administrative roles for the correct configuration, maintenance, and administration of the cryptographic module

[SOURCE: ISO/IEC 19790:2012, 3.2]

**3.3**
**application environment**
set of all software and hardware consisting of an operating system and hardware platform required for an application, which will call a cryptographic module for services, to operate securely

Note 1 to entry: The application environment may be identical to the operational environment (e.g. both the crypto module and application are executing in the same environment).

**3.4**
**competence**
ability to apply knowledge and skills to achieve intended results

Note 1 to entry: It represents the set of knowledge, skill, and effectiveness needed to carry out the job activities associated with one or more roles in an employment position.

[SOURCE: ISO/IEC 17024:2012, 3.6, modified — Note 1 to entry has been added,]

**3.5**
**critical security parameter**
**CSP**
security-related information whose disclosure or modification can compromise the security of a cryptographic module

EXAMPLE Secret and private cryptographic keys, authentication data such as passwords, PINs, certificates or other trust anchors.

Note 1 to entry: A CSP can be plaintext or encrypted.

[SOURCE: ISO/IEC 19790:2012, 3.18]

**3.6**
**cryptographic algorithm**
well-defined computational procedure that takes variable inputs, which may include cryptographic keys, and produces an output

[SOURCE: ISO/IEC 19790:2012, 3.20]

**3.7**
**cryptographic module**
**CM**
**module**
set of hardware, software, and/or firmware that implements security functions and are contained within the cryptographic boundary

[SOURCE: ISO/IEC 19790:2012, 3.25, modified — CM has been added as an admitted term.]

**3.8**
**cryptographic module security policy**
**security policy**
precise specification of the security rules under which a *cryptographic module* (3.7) shall operate, including the rules derived from the requirements specified in ISO/IEC 19790:2012, Annex B and additional rules imposed by the module or *validation authority* (3.22)

[SOURCE: ISO/IEC 19790:2012, 3.26, modified — In the definition, "this document" has been changed to reference ISO/IEC 19790.]

**3.9**
**non-administrator guidance**
written material that is used by the *users* (3.20) and/or other non-administrative roles for operating the *cryptographic module* (3.7) in an approved mode of operation

Note 1 to entry: The non-administrator guidance describes the security functions of the cryptographic module and contains information and procedures for the secure use of the cryptographic module, including instructions, guidelines, and warnings.

[SOURCE: ISO/IEC 19790:2012, 3.77]

**3.10**
**operational environment**
set of all software and hardware consisting of an operating system and hardware platform required for the module to operate securely

[SOURCE: ISO/IEC 19790:2012, 3.83]

**3.11**
**operational tester**
**tester**
individual assigned by an *organization* (3.15) to perform test activities in accordance with the *operational testing process* (3.13)

**3.12**
**operational testing**
**OT**
test to determine the correct installation, configuration and operation of a module and that it operates securely in the *operational environment* (3.10)

**3.13**
**operational testing process**
**OTP**
process to support determining the correct installation, configuration and operation of a module and that it operates securely in the *operational environment* (3.10)

**3.14**
**operator**
individual or a process (subject) operating on behalf of the individual, authorized to assume one or more roles

[SOURCE: ISO/IEC 19790:2012, 3.85]

**3.15**
**organization**
entity specifying, deploying and operating a *cryptographic module* (3.7)

**3.16**
**pre-operational test**
*operational testing* (3.12) to be performed by a *vendor* (3.23) during the development of a *cryptographic module* (3.7) or on behalf of a *validation authority* (3.22) during the validation under ISO/IEC 19790:2012 for the intended *operational environment* (3.10)

**3.17**
**public security parameter**
**PSP**
security-related public information whose modification can compromise the security of a *cryptographic module* (3.7)

EXAMPLE Public cryptographic keys, public key certificates, self-signed certificates, trust anchors, one-time passwords associated with a counter and internally held date and time.

Note 1 to entry: A PSP is considered protected if it cannot be modified or if its modification can be determined by the module.

[SOURCE: ISO/IEC 19790:2012, 3.99]

**3.18**
**random bit generator**
**RBG**
device or algorithm that outputs a sequence of bits that appears to be statistically independent and unbiased

[SOURCE: ISO/IEC 19790:2012, 3.100]

**3.19**
**sensitive security parameter**
**SSP**
*critical security parameters (CSP)* (3.5) and *public security parameters (PSP)* (3.17)

[SOURCE: ISO/IEC 19790:2012, 3.110]

**3.20**
**user**
role taken by an individual or process (i.e. subject) acting on behalf of an individual that accesses a *cryptographic module* (3.7) in order to obtain cryptographic services

[SOURCE: ISO/IEC 19790:2012, 3.130]

**3.21**
**validated**
assurance of tested conformance by a *validation authority* (3.22)

[SOURCE: ISO/IEC 19790:2012, 3.131]

**3.22**
**validation authority**
entity that will validate the testing results for conformance to an International Standard

[SOURCE: ISO/IEC 19790:2012, 3.132, modified — In the definition, “this” has been changed to “an”.]

**3.23**
**vendor**
entity, group or association that submits the *cryptographic module* (3.7) for testing and validation

Note 1 to entry: The vendor has access to all relevant documentation and design evidence regardless if they did or did not design or develop the cryptographic module.

[SOURCE: ISO/IEC 19790:2012, 3.133]

## 4 Abbreviated terms

The abbreviated terms given in ISO/IEC 19790:2012, Clause 4 apply.

## 5 Document organization

Clause 6 describes the context of operational testing in an organization’s environment and the relationships with other key stakeholders in the production and specification of cryptographic modules.

Clause 7 specifies the types of cryptographic modules, security requirements, life-cycle assurance, security policy requirements and guidance, and intended purpose that should be satisfied by the cryptographic module’s compliance to ISO/IEC 19790.

Clause 8 describes the operational environment which cryptographic modules are utilized in and security requirements related to cryptographic modules for their operational environment.

Clause 9 provides guidance on how to select cryptographic modules in their operational environment.

Clause 10 describes the principles for operational testing, including the assumptions to be made testing activities to be performed, expected competence requirements of operational testers, use of evidences that has been gained from the validation of cryptographic modules, documentation requirements for operational testing, and procedures for operational testing.

Clause 11 describes the principles for operational testing including:

- assessing the installation, configuration, and operation;
- identifying the residual vulnerabilities;
- inspecting the key management system;
- inspecting the security requirements of authentication credentials;
- assessing the availability of cryptographic modules;
- checking the security policies.

Clause 12 describes how to report the results of operational testing, describing the contents of a report giving the results of operational testing.

## 6 Context of operational testing

A vendor designs, develops and manufactures a cryptographic module. The vendor may have the module validated by a validation authority in support of a claim that the module is compliant to ISO/IEC 19790.

NOTE For some organizations, there can be an organizational security policy such that the module validated by a named validation authority can be acquired by an organization for deployment in a security system or application environment.

Figure 1 shows the scope of this document in context with a generalized life-cycle of a cryptographic module. It depicts both the development life-cycle of the module by the vendor, and the life-cycle of the module in the organization’s environment.

The vendor starts with a risk assessment process to determine the security requirements for cryptographic modules. This risk assessment, which is based on the intended operational environment and the intended market, defines the modules security requirements for each specific area in ISO/IEC 19790. Once defined, the vendor proceeds with the module's development which includes the design, implementation and testing processes.

Typically, validation by a validation authority, is initiated by the vendor, but validation can also be initiated by an original equipment manufacturer, an integrator, or by the organization itself.

An organization performs a risk assessment and defines security requirements for their operational environment. To address this risk assessment, the organization may procure a validated cryptographic module which satisfies the security requirements, and performs the operational testing process, before the module is deployed. The cryptographic modules reflected by their assurance maintenance should be used in operational testing.

The operational testing process, as shown in Figure 1, is performed to select a proper cryptographic module for use in a specific operational environment. The result of the operational testing process may be used to perform the organization’s accreditation of the cryptographic module.

The operational testing process is located between module's validation and organization accreditation. The scope of this document is the operational testing process, shown in Figure 1 as a gray box.

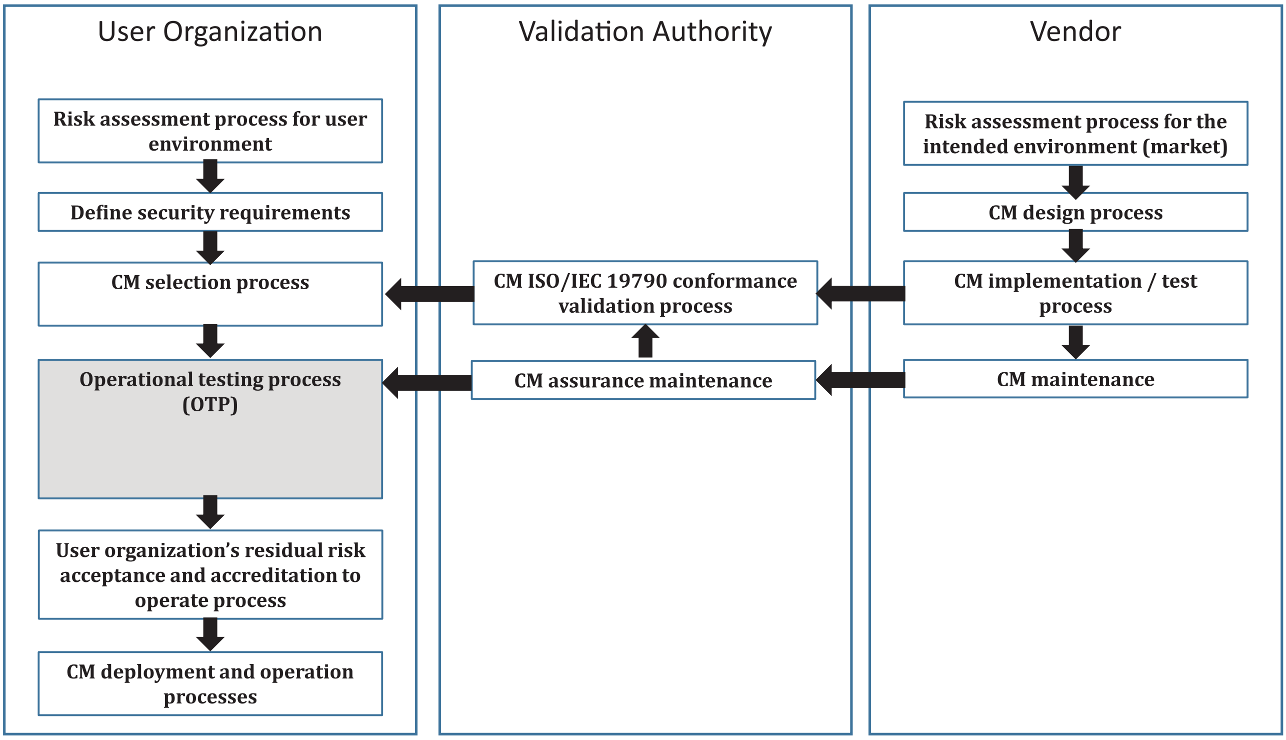
User Organization
Risk assessment process for user environment
Define security requirements
CM selection process
Operational testing process (OTP)
User organization's residual risk acceptance and accreditation to operate process
CM deployment and operation processes
Validation Authority
CM ISO/IEC 19790 conformance validation process
CM assurance maintenance
Vendor
Risk assessment process for the intended environment (market)
CM design process
CM implementation / test process
CM maintenance

**Figure 1 — Process for developing, validating, accreditation, deploying and operation of a cryptographic module**

# 7 Cryptographic modules

## 7.1 General

This clause specifies the types of cryptographic modules, security requirements, life-cycle assurance, security policy requirements and guidance, and intended purpose that are satisfied when a cryptographic module is in compliance with ISO/IEC 19790.

The vendor provides the security policy document and the required guidance that is specified in ISO/IEC 19790. The vendor may also provide other documentation, guidance, tools or specifications that were not specified as part of the compliance with ISO/IEC 19790.

## 7.2 Types of cryptographic modules

### 7.2.1 General

Cryptographic modules can take various forms of modules as illustrated in Figure 2, and contain various kinds of security functions, different security function strengths, etc. Cryptographic modules may contain the same algorithms with appropriate security strengths.

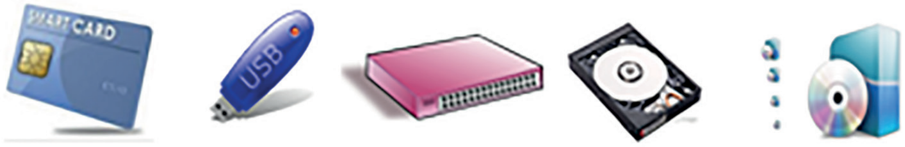

**Figure 2 — Various types of cryptographic modules**