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.

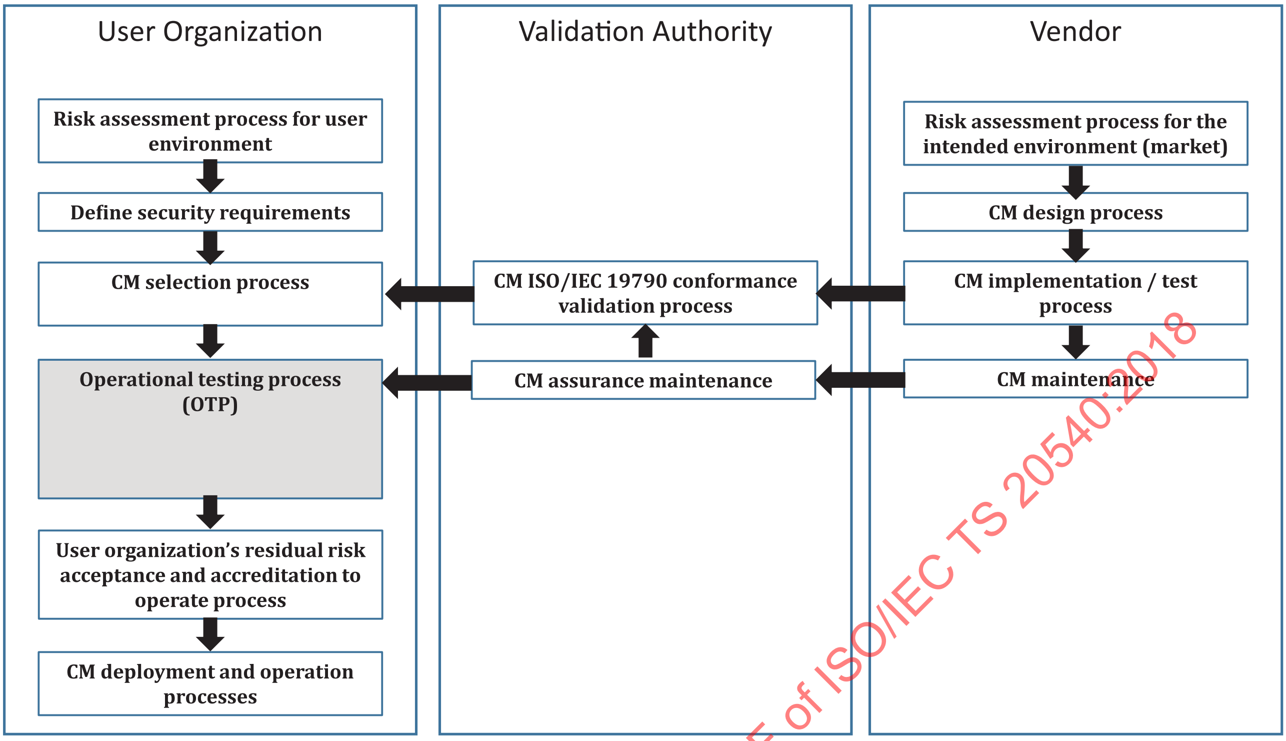
User Organization
Risk assessment process for user environment
Define security requirements
CM selection process
Operational testing process (OTP)
User organization's residual risk acceptance and accreditation to operate process
CM deployment and operation processes
Validation Authority
CM ISO/IEC 19790 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.

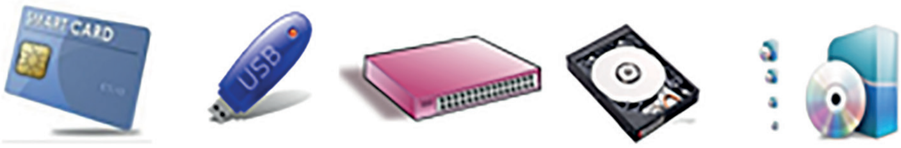

Figure 2 — Various types of cryptographic modules

The following cryptographic module types are defined by ISO/IEC 19790: software cryptographic module, firmware cryptographic module, hardware cryptographic module, and hybrid cryptographic module. Precise descriptions of the types of cryptographic modules are given in ISO/IEC 19790:2012, 7.2.2, and are reproduced below.

7.2.2 Software module

A software module is a module whose cryptographic boundary delimits the software exclusive component(s) (can be one or multiple software components) that execute(s) in a modifiable operational environment. The computing platform and operating system of the operational environment which the software executes in are external to the defined software module boundary.

The maximum overall security rating of software module is Security Level 2.

7.2.3 Firmware module

A firmware module is a module whose cryptographic boundary delimits the firmware exclusive component(s) that execute(s) in a limited or non-modifiable operational environment. The computing platform and operating system of the operational environment which the firmware executes in are external to the defined firmware module boundary but explicitly bound to the firmware module.

The maximum overall security rating of firmware module is Security Level 4.

7.2.4 Hardware module

A hardware module is a module whose cryptographic boundary is specified at a hardware perimeter. Firmware and/or software, which may also include an operating system, may be included within this hardware cryptographic boundary.

The maximum overall security rating of hardware module is Security Level 4.

7.2.5 Hybrid software module

A hybrid software module is a module whose cryptographic boundary delimits the composite of a software component that executes in a modifiable operational environment and a disjoint hardware component (i.e. the software component is not contained within the hardware module boundary). The computing platform and operating system of the operational environment which the software executes in are external to the defined hybrid software module boundary.

The maximum overall security rating of hybrid software module is Security Level 2.

7.2.6 Hybrid firmware module

A hybrid firmware module is a module whose cryptographic boundary delimits the composite of a firmware component that executes in a limited or non-modifiable operational environment and a disjoint hardware component (i.e. the firmware component is not contained within the hardware module boundary). The computing platform and operating system of the operational environment which the firmware executes in are external to the defined hybrid firmware module boundary but explicitly bound to the hybrid firmware module.

The maximum overall security rating of hybrid firmware cryptographic module is Security Level 4.

7.3 Cryptographic module application environments

Cryptographic modules are used in context with a wide spectrum of data sensitivities (e.g. low value administrative data, million-dollar funds transfer, life protecting data, personal identity information, and sensitive information used by government) and in a diverse set of application environments (e.g. a guarded facility, and office, removable media, and completely unprotected location) as Figure 3.

Figure 3 — A diverse set of application environments

7.4 Security products with cryptographic modules

Vendors develop and market products that include cryptographic functionality. A product may be a cryptographic module whose boundary is identical to the validated module. A product may incorporate an embedded validated cryptographic module in addition to other functionalities. Therefore, the boundary of the product is not the same boundary as the validated cryptographic module.

A cryptographic module may be composed of validated cryptographic modules. A product may incorporate the composition of validated cryptographic modules in addition to other functionalities. Figure 4, below describes the various composition types of the cryptographic modules. The composition types are classified as modules included by the component, modules connected in the network, and modules composed by layering.

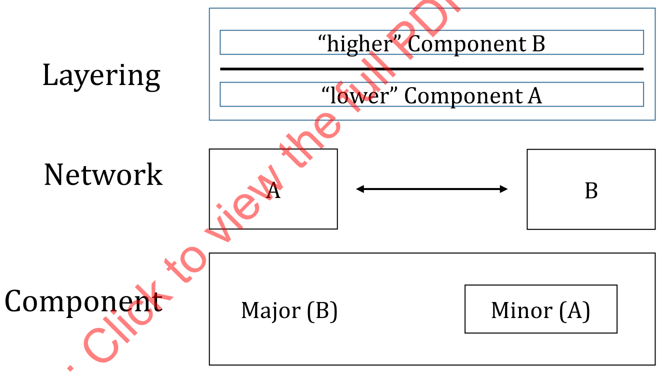

Figure 4 — Types of composition of cryptographic modules

If the product consists only of the validated modules, the organization can verify the validation against the validation authorities listing of validated modules by comparing the versioning information provided with the module's documentation from the vendor and by directly querying the module (see ISO/IEC 19790:2012 7.2.3.1 and 7.4.3.1).

It can be difficult to perform such verification of the validated module if it is an embedded component within a larger product. The vendor should provide product documentation that includes references to the versioning information for the embedded validated cryptographic module. The product should also provide a mechanism for the user to query the embedded validated module to determine the embedded module's versioning information. When the validated cryptographic module is part of a larger product boundary, there is no validation authority assurance on the correct operation of the larger product utilizing the embedded module. The vendor should provide a statement of assurance that all the cryptographic functionality within the product boundary is provided solely by the embedded validated cryptographic modules.

If a product contains a composite of a validated cryptographic module which implements approved security functions and a non-validated cryptographic module which implements non-approved security functions (e.g. key establishment, key storage etc.), and the security services provided by the module are a composite of the two embedded modules, the organization should recognize that the product service can be approved or not. If the organization utilizes non-approved security services, the operational environment can create a risk to operational security.

EXAMPLE 1 If data is encrypted by the non-validated module, and then encrypted by the validated module, the composite result can be considered approved.

EXAMPLE 2 If a security function on the validated module utilizes key establishment function from the non-validated module, the composite result can be considered non-approved.

If a product contains multiple cryptographic modules, each individual module's versioning information should be verified separately against the validation authorities' list of validated modules.

If the validated cryptographic module is a component of a larger product which contains many components (i.e. non-security components and security components), the vendor documentation should provide information on how to assemble or compose the components together correctly.

If the validated cryptographic module is distributed as open source code, the module's security policy document provides information to verify the integrity of the source code files and specify the compilers and control parameters required to compile the code into an executable format (see ISO/IEC 19790:2012, B.2.5).

7.5 Security requirements for cryptographic modules

7.5.1 General

The security requirements for cryptographic modules are specified in ISO/IEC 19790. There are 11 security areas in the security requirements. These areas include cryptographic module specification; cryptographic module interfaces; roles, services, and authentication; software/firmware security; operational environment; physical security; non-invasive security; sensitive security parameter management; self-tests; life-cycle assurance; and mitigation of other attacks.

Four security levels are specified for each of the 11 requirement areas. Each security level offers an increase in security over the preceding level. The cryptographic module is independently rated in each area. Several areas provide for increasing levels of security with cumulative security requirements for each security level. In these areas, the cryptographic module receives a rating that reflects the highest-security level for which the module fulfils all the requirements of that area. In areas that do not provide for different levels of security, the cryptographic module receives a rating commensurate with the overall rating.

In addition to receiving independent ratings for each of the security areas, a cryptographic module also receives an overall security rating. The overall security rating indicates the minimum level of the independent ratings received in the areas.

The four increasing levels of security allow cost-effective solutions that are appropriate for different degrees of data sensitivity and different application environments.

Subclauses 7.5.2 to 7.5.5 provide an overview of the four security levels. The cryptographic techniques (e.g. cryptographic algorithms, security functions, etc.) are identical over the four security levels. Each security level levies increasing levels of security requirements for the protection of the module itself (e.g. access and knowledge of internal components and operation) and SSPs contained and controlled within the module.

7.5.2 Security Level 1

Security Level 1 provides a baseline level of security. Basic security requirements are specified for a cryptographic module (e.g. at least one approved security function or approved sensitive security parameter establishment method should be used). Software modules operate in a modifiable operating environment and firmware modules operate in a limited or non-modifiable operating environment. No specific physical security mechanisms are required in a Security Level 1 hardware cryptographic module beyond the basic requirement for production-grade components. Non-invasive mitigation methods or mitigation of other attacks which are implemented are documented. Examples of a Security Level 1 cryptographic module is a hardware encryption board found in a personal computer (PC) or a cryptographic toolkit executing in a handheld device or general-purpose computer.

Such implementations are ideally appropriate for security applications where controls, such as physical security, network security, and administrative procedures are provided outside of the module but within the environment which it is to be deployed. For example, the implementation of Security Level 1 cryptographic module can be more cost-effective in such environments than corresponding modules at higher security levels which provide greater security of the modules SSPs, enabling organizations to select alternative cryptographic solutions to meet security requirements where attention to the environment the module is operating is crucial in providing overall security.

7.5.3 Security Level 2

Security Level 2 enhances the physical security mechanisms of Security Level 1 by adding the requirement for tamper-evidence, which includes the use of tamper-evident coatings or seals or pick-resistant locks on removable covers or doors.

Tamper-evident coatings or seals are placed on a module so that the coating or seal should be broken to attain physical access to SSPs within the module. Tamper-evident seals or pick-resistant locks are placed on covers or doors to protect against unauthorized physical access.

Security Level 2 requires role-based authentication in which a cryptographic module authenticates the authorization of an operator to assume a specific role and perform a corresponding set of services.

Security Level 2 allows a software cryptographic module to be executed in a modifiable environment that implements role-based access controls or, at the minimum, a discretionary access control with robust mechanism of defining new groups and assigning restrictive permissions through access control lists (e.g. Access Control Lists), and with the capability of assigning each user to more than one group, and that protects against unauthorized execution, modification, and reading of cryptographic software.

7.5.4 Security Level 3

In addition to the tamper-evident physical security mechanisms required at Security Level 2, Security Level 3 provides additional requirements to mitigate the unauthorized access to SSPs held within the cryptographic module. Physical security mechanisms required at Security Level 3 are intended to have a high probability of detecting and responding to attempts at direct physical access, use or modification of the cryptographic module and probing through ventilation holes or slits. The physical security mechanisms may include the use of strong enclosures and tamper detection/response circuitry that zeroize all CSPs when the removable covers/doors of the cryptographic module are opened.

Security Level 3 requires identity-based authentication mechanisms, enhancing the security provided by the role-based authentication mechanisms specified for Security Level 2. A cryptographic module authenticates the identity of an operator and verifies that the identified operator is authorized to assume a specific role and perform a corresponding set of services.

Security Level 3 requires manually established plaintext CSPs to be encrypted, utilize a trusted channel or use a split knowledge procedure for entry or output.

Security Level 3 also protects a cryptographic module against a security compromise due to environmental conditions outside of the module's normal operating ranges for voltage and temperature. Intentional excursions beyond the normal operating ranges can be used by an attacker to thwart a cryptographic module's defences. A cryptographic module is required to either include special environmental protection features designed to detect when the voltage and temperature boundaries are exceeded and zeroize CSPs, or to undergo rigorous environmental failure testing to provide a reasonable assurance that the module is not affected when outside of the normal operating range in a manner that can compromise the security of the module.

Non-invasive mitigation methods specified in ISO/IEC 19790:2012, 7.8 which are implemented in the module are tested at Security Level 3 metrics.

Security Level 3 is not offered in all clauses of ISO/IEC 19790 for software cryptographic modules. Therefore, the overall highest security level achievable by software cryptographic module is limited to Security Level 2.

Security Level 3 modules require additional life-cycle assurances, such as automated configuration management, detailed design, low-level testing, and operator authentication using vendor-provided authentication information.

7.5.5 Security Level 4

Security Level 4 provides the highest level of security defined in ISO/IEC 19790. This level includes all the appropriate security features of the lower levels, as well as extended features.

At Security Level 4, the physical security mechanisms provide a complete envelope of protection around the cryptographic module with the intent of detecting and responding to all unauthorized attempts at physical access when SSPs are contained in the module whether external power is applied or not. Penetration of the cryptographic module enclosure from any direction has a very high probability of being detected, resulting in the immediate zeroization of all unprotected SSPs. Security Level 4 cryptographic modules are useful for operation in physically unprotected environments.

Security Level 4 introduces the multi-factor authentication requirement for operator authentication. At minimum, this requires two of the following three attributes:

a) something known, such as a secret password;

b) something possessed, such as a physical key or token;

c) a physical property, such as a biometric.

At Security Level 4 a cryptographic module is required to include special environmental protection features designed to detect voltage and temperature boundaries and zeroize all unprotected SSPs to provide a reasonable assurance that the module is not affected when outside of the normal operating range in a manner that can compromise the security of the module.

Non-invasive mitigation methods specified in ISO/IEC 19790:2012, 7.8 which are implemented in the module are tested at Security Level 4 metrics.

Security Level 4 is not offered in all clauses of ISO/IEC 19790 for software cryptographic modules.

The design of a Security Level 4 module is verified by the correspondence between both pre- and post-state conditions and the functional specification.

7.6 Life-cycle assurance of cryptographic modules

ISO/IEC 19790:2012, 7.11 refers to the validation requirements of the vendor of a cryptographic module during the design, development, vendor testing, delivery, operation and end of life, providing assurance that the module is properly designed, developed and that vendor testing, delivery, and operation and end of life requirements are properly performed. Guidance documentation is also specified as both administrator and non-administrator guidance. ISO/IEC 19790:2012, 7.11 also addresses the vendor's configuration management and finite state model requirements.

The operational tester should inspect ISO/IEC 19790:2012, 7.11 and use this information to properly install, configure and test the modules in their operational environment.

7.7 Cryptographic module security policy

7.7.1 General

The vendor should provide cryptographic security policy requirements related to the cryptographic module as specified in ISO/IEC 19790:2012, Annex B. The validation of the module addresses the conformance of the vendor provided security policy, as applicable, to this set of requirements. The operational tester may use the security policy.

NOTE Annex B provides an example of a checklist that consolidates the lists given in this document.

7.7.2 Cryptographic module specification

- Illustrative diagram schematic and photograph of the module.
- Description of module, including clear and non-ambiguous reference of the hardware and software versioning.
- Module's cryptographic boundaries.
- Modes of operation.
- Degraded operation.
- Security functions.
- Overall security design.
- Security and non-security services.
- Approved and non-approved security services.

7.7.3 Cryptographic module interfaces

- Listing of all ports and interfaces (physical and logical).
- Information passing over the logical interfaces.
- Physical ports and data that pass over them.
- Trusted channel.

7.7.4 Roles, services, and authentication

- All roles, with corresponding service commands with input and output.
- Each authentication method.
- Strength of authentication requirement.
- Two independent actions in case of having a self-initiated cryptographic output capability.
- Controls on loading and isolation of code that deter unauthorized access to and use of the module in case of loading external software or firmware.
- All services.

7.7.5 Software/firmware security

- Approved integrity techniques.
- Form and each component of executable code provided.
- Compilers and control parameters required to compile the code into an executable format in case that the module is open source.

7.7.6 Operational environment

- Operational environment: non-modifiable, limited, and modifiable.
- Expected operating system and tested platform(s).
- Description of how requirements are satisfied.
- Specification of the security rules, settings or restrictions to the configuration of the operational environment.
- Specification of any restrictions to the configuration of the operational environment.

7.7.7 Physical security

- Embodiment: single-chip, multi-chip embedded or multi-chip standalone.
- Physical security mechanisms (e.g., tamper evident seals, locks, tamper response and zeroization switches, and alarms).
- Specification of the actions required by the operator(s) to ensure that the physical security is maintained (e.g., periodic inspection of tamper-evident seals or testing of tamper response and zeroization switches).
- Fault induction mitigation methods implemented.

7.7.8 Non-invasive security

- All non-invasive mitigation techniques.
- Effectiveness of the non-invasive mitigation techniques.

ISO/IEC 17825 should be considered and referenced.

7.7.9 Sensitive security parameters management

- Key list specifying the type(s), strength(s) in bit, security function(s), and security function certification number(s), where and how the key(s) is generated, whether the key(s) is imported or exported, and establishment method used.
- Other SSPs and how they are generated.
- Uses of RBG output(s).
- RBG entropy source(s).
- Electronic and manual key I/O method(s).
- SSP storage technique(s).
- Unprotected SSP zeroization method(s) and rationale, and operator initiation capability.
- Applicable transition periods or timeframes where an algorithm or key length transitions from approved to non-approved.

7.7.10 Self-tests

- Pre-operational and conditional self-tests with defined parameters.
- Conditions under which the self-test are performed.

- Time period and policy regarding any conditions that can result in the interruption of the module’s operations during the time to repeat the period self-tests.
- All error states and status indicators.
- Operation initiation, if applicable.

7.7.11 Life-cycle assurance

- Procedures for secure installation, initialization, start-up and operation of the module.
- Maintenance requirements.
- Administrator and non-administrator guidance.

7.7.12 Mitigation of other attacks

- Techniques to mitigate other attacks.
- Effectiveness of the mitigation techniques.
- Security-relevant guidance and constraints.

The level of detail describing the security mechanism(s) implemented to mitigate other attacks should be similar to what is found on advertisement documentation (product glossies).

7.8 Intended purpose of validated cryptographic modules

This subclause describes the intended purpose of the cryptographic module.

The security levels of ISO/IEC 19790 are focused on the protection of the modules CSPs by the module itself, regardless of the environment the module is deployed in. Therefore, selection of a security level is greatly influenced by the environment the module is to be deployed.

The overall security level of a cryptographic module should be chosen to provide a level of security appropriate for the security requirements of the operational environment in which the module is to be utilized and for the security services that the cryptographic module is to provide according to the intended purpose of the cryptographic module.

If the intended environment is different from the organization’s operational environment, it is possible that the intended purpose of a validated cryptographic module in a computer or telecommunications system is not sufficient to ensure the security of the overall system.

The responsible authority in each organization should ensure that their computer and telecommunication systems that utilize cryptographic modules provide an acceptable level of security for the given operational environment.

The importance of security awareness and of making information security a management priority should be communicated to all users. Since information security requirements vary for different operationals, organizations should identify their information resources and determine the sensitivity to and the potential impact of losses. Controls should include administrative policies and procedures, physical and environmental controls, information and data controls, software development and acquisition controls, and backup and contingency planning.

A computer or telecommunication system can contain multiple instances of the same cryptographic module or multiple instances of different cryptographic module (e.g., multiple cryptographic modules provided by several different vendors or of different functional attributes).

8 The application environment

8.1 Organizational security

As the security levels of ISO/IEC 19790 are focused on the protection of the cryptographic modules CSPs by the module itself regardless of the environment the module is deployed in, organizations should identify their information resources and determine the sensitivity and the potential impact of loss of CSPs in the operational and application environments.

The responsible authority in each organization should ensure that the computer and telecommunication systems that utilize cryptographic modules provide an acceptable level of security for the given application environment. Since each organization is responsible for selecting which approved security functions are appropriate for a given application, the organization should be aware that conformance with ISO/IEC 19790 does not imply full interoperability of compliant products. The importance of security awareness, including relevant security policies, and making information security a management priority should be communicated to all concerned.

Organizations should identify their administrative policies and procedures, physical and environmental controls, information and data controls, software development and acquisition controls, and backup and contingency planning.

There should be:

- management policies, rules and procedures that govern operation of the application environment;
- requirements and rules for interaction between both trusted and untrusted systems in the application environment;
- technical controls, operational controls and management controls to maintain the security of the application environment. ISO/IEC 27002 provides security controls often specified by an organization.

8.2 Architecture of the application environment

Logically, all the portions of the system under the same set of security policies, security requirements and security documentation can be termed a security domain.

A security domain can offer security services that can be used by other domains through communications or application programming interfaces.

It is possible that some security domains can require differing security levels or cryptographic algorithm strengths.

A security system which utilizes cryptographic modules can decompose a subsystem which is a set of one or more operational components that are capable of execution independently from the rest of the security system. An operational component implements part of the system's functionality (whether security related or not).

When designing the architecture of the application environment, an organization should consider the following.

- Since each organization is responsible for selecting which approved security functions are appropriate for a given application, the organization should be aware that conformance with ISO/IEC 19790 does not imply full interoperability of compliant products.
- The application environment can have security policies that apply to some security domains while not applying to others.
- All interfaces between the operational system and its application environment need to be defined.

9 The operational environment

9.1 Security requirements related to cryptographic modules for their operational environment

9.1.1 General

Security requirements related to cryptographic modules which are required in their operational environment are specified in the specification for the operational environment which the cryptographic modules are to be deployed. The organization has the responsibility to create the specification for the operational environment throughout cryptographic module risk assessment process for the environment and defining security requirements as illustrated in Figure 1.

Security requirements for the operational environment can be presented as two types; those that are supported by the cryptographic module and those supported by the operational environment.

9.1.2 Entropy sources

If cryptographic modules need entropy sources which are used as the seed of random bit generator, and the entropy sources are collected in the operational environment, the entropy sources should satisfy the requirements for the strength of cryptographic algorithms and security requirements which are described in ISO/IEC 20543.

9.1.3 Audit mechanism

If cryptographic modules utilize an audit mechanism which is implemented in the operational environment, then the audit mechanism should satisfy the security requirements for ISO/IEC 19790.

9.1.4 Physically unclonable function

If cryptographic modules need a physically unclonable function for generating nonstored security parameters in the operational environment, it should satisfy the requirements for the strength of cryptographic algorithms and security requirements which are described in ISO/IEC 20897.

9.2 Security assumptions for the operational environment

9.2.1 General

Subclause 7.5 identifies requirements for four security levels for cryptographic modules to provide for a wide spectrum of data sensitivity (e.g., low value administrative data, million-dollar funds transfers, and life protecting data) and a diversity of application environments (e.g., a guarded facility, an office, and a completely unprotected location).

These four increasing levels of security allow cost-effective solutions that are appropriate for different degrees of data sensitivity and different application environments.

The use of a validated cryptographic module in a computer or telecommunications system is not sufficient to ensure the security requirements of the overall system. The overall security level of a cryptographic module should be chosen to provide a level of security appropriate for the security requirements of the application and operational environment in which the module is to be utilized and for the security services that the module is to provide. The responsible authority in each organization should ensure that their computer and telecommunication systems that utilize cryptographic modules provide an acceptable level of security for the given application and operational environment.

The importance of security awareness and of making information security a management priority should be communicated to all users. Since information security requirements vary for different applications, organizations should identify their information resources and determine the sensitivity to and the potential impact of losses. Controls should be based on the potential risks and should be selected from available controls, including administrative policies and procedures, physical and environmental controls, information and data controls, software development and acquisition controls, and backup and contingency planning.

The four security levels of ISO/IEC 19790 are focused on the protection of the modules CSPs by the module itself, regardless of the environment the module is deployed in. Therefore, selection of a security level is greatly influenced by the environment in which the module is to be deployed. For example, a Level 1 security level, which does not itself provide physical security protection, can be an acceptable solution in some security systems because the environment provides the required physical security protection features.

Subclauses 9.2.2 to 9.2.4 define security assumptions for the cryptographic module. This information is provided from Reference [9] in the Bibliography.

NOTE Annex B provides an example of a checklist that consolidates the lists given in this document.

9.2.2 Security Level 1

Protection provided:

No physical protection of CSPs provided by the module; access assumed

- Hardware: probing and observation of components assumed.
- Software: access to operating environment, applications and data assumed.

NOTE The module can employ non-invasive mitigation methods.

Assumptions:

- Correct operation of the Approved cryptographic services and security functions;
- All attacks result in access to CSPs and data (plaintext and ciphertext) held within the module;
- Operator is responsible for the physical protection of the module; and
- Value or sensitivity of data protected by the module is assumed negligible in an unprotected environment.

Attack type:

Passive attack to gain immediate access to CSPs and data held by the module.

Attack characterization/testing assumptions:

- No prior access to the module is assumed.
- No tools and materials are assumed needed.

Value:

The module provides correct operation of security functions and services. Protection of the plaintext CSPs and data held within the module is provided by the operator of the module (e.g. the environment the module can be used). If the module is used in an unprotected environment, then the module should not hold or maintain unprotected plaintext CSPs or data.

9.2.3 Security Level 2

Protection provided:

- Observable evidence of tampering.

- Physical boundary of the module is opaque to prevent direct observation of internal security components.
- Hardware: probing is assumed.
- Software: logical access protection of the cryptographic modules unprotected CSPs and data is provided by the operating system satisfying the security requirements which are specified in ISO/IEC 19790:2012 7.6.3.

NOTE The module can employ non-invasive mitigation methods.

Assumptions:

- Correct operation of the Approved cryptographic services and security functions;
- All attacks result in access to CSPs and data (plaintext and ciphertext) held within the module;
- Operator is responsible for the physical protection of the module; and
- Value or sensitivity of data protected by the module is assumed low in an unprotected environment.

Attack type:

Active attack to gain immediate access to CSPs and data held by the module.

Attack characterization/testing assumptions:

- No prior access to the module is assumed.
- Readily available low-cost tools and materials which are on hand at time of attack.
- Attack time is assumed to be low.

Value:

The module provides correct operation of security functions and services. Protection of the plaintext CSPs and data held within the module is provided by the operator of the module (e.g. the environment the module can be used). The operator of the module is aware by tamper evidence that internal information can be compromised. If the module is used in an unprotected environment, then the module should not hold or maintain unprotected plain-text CSPs or data which have a moderate or high value.

9.2.4 Security Level 3

Protection provided:

- Observable evidence of tampering.
- Physical boundary of the module is opaque to prevent direct observation of internal security components.
- Direct entry/probing attacks prevented.
- Strong tamper resistant enclosure or encapsulation material.
- If applicable, active zeroization if covers or doors opened.
- Software: non-applicable

NOTE The module can employ non-invasive mitigation methods.

Assumptions:

- Correct operation of the Approved cryptographic services and security functions;

- When attacker has physical access or proximity to the module, non-direct attacks can result in access to CSPs and data (plaintext and ciphertext) held within the module; and
- Value of data protected by the module is assumed moderate in an unprotected environment.

Attack type:

Moderately aggressive attack to gain immediate access to CSPs and data held by the module.

Attack characterization/testing assumptions:

- Prior access to or basic knowledge of the module is assumed.
- Readily available tools and materials.
- Actual attack time is assumed to be moderate (this does not include time spend gaining prior access or basic knowledge of module).

Value:

The module provides correct operation of security functions and services. Protection of the plaintext CSPs and data held within the module is provided by the operator of the module (e.g. the environment the module can be used) and by the physical protection mechanisms of the module (e.g. strong enclosure, tamper response for covers and doors, deterrent of probing, EFP or EFT for temperature and voltage, mitigation against non-invasive attack). The operator of the module is aware by tamper evidence that internal information can be compromised. An attack is pre-meditated but is of moderate difficulty. If the module is used in an unprotected environment, then the module should not hold or maintain unprotected plain-text CSPs or data which have a high value.

9.2.5 Security Level 4

Protection provided:

- Observable evidence of tampering.
- Physical boundary of the module is opaque to prevent direct observation of internal security components.
- Direct entry/probing attacks prevented.
- Strong tamper resistant enclosure or encapsulation material.
- If applicable, active zeroization if covers or doors opened.

NOTE The module can employ non-invasive mitigation methods.

A complete envelope of protection around the module preventing unauthorized attempts at physical access.

- Penetration of the module's enclosure from any direction had a very high probability of being detected resulting in immediate zeroization of plaintext CSPs or severe damage to the module rendering it inoperable.
- When attacker has physical access or proximity to the module, the module prevents access to CSPs and data (plaintext and ciphertext) held within the module from non-direct attacks.
- Software: non-applicable

Assumptions:

- Correct operation of the Approved cryptographic services and security functions;
- Module is tamper resistant against all physical attacks defined in ISO/IEC 19790; and

- Value of data protected by the module is assumed high in an unprotected environment.

Attack type:

Aggressive attack to gain immediate access to CSPs and data held by the module.

Attack characterization/testing assumptions:

- Prior access to or advanced knowledge of the module is assumed.
- Specialized tools and materials.
- Temperature and voltage attacks.
- No time restriction on attack.

Value:

The module provides correct operation of security functions and services. Protection of the plaintext CSPs and data held within the module is provided by the operator of the module (e.g. the environment the module can be used) and by the physical protection mechanisms of the module (e.g. strong enclosure, tamper response for covers and doors, complete envelope of protection and penetration detection resulting in immediate zeroization of plaintext CSPs, EFP for voltage and temperature, mitigation against non-invasive attack, protection from fault induction). The operator of the module is aware by tamper evidence that the module was attached. The module should zeroize all unprotected CSPs before an attacker can compromise the module. An attack is pre-meditated, well-funded, organized and determined.

10 How to select cryptographic modules

10.1 General

This clause provides guidance on selecting a cryptographic module. The organization selects the cryptographic modules which satisfies the organization's security requirements for the operational environment. Once selected, the same cryptographic module and operational environment is used to perform the module’s operational testing.

10.2 Use policy

Before a cryptographic module can be selected, the organization should determine which data needs cryptographic protection, where that cryptographic protection needs to be provided and the security strength, algorithms and protocols to be utilized for that cryptographic protection. The determination is dependent on the use case.

Examples of data to be considered for cryptographic protection:

- Personal Identity Information (PII);
- Business Identity Information (BII);
- Communications;
- Data at rest;
- Other sensitive information.

Examples of where data may require cryptographic protection:

- Data storage:
  - Archival data;

  - Operational data;
- Data in transit:
  - Client to client (e.g. VPN, end to end encryption mechanisms, etc.);
  - LAN;
  - WAN;
  - Wireless:
    - Wi-Fi;
    - Bluetooth;
    - Radio;
    - Satellite telemetry;
  - Removable media:
    - Memory cards;
    - USB storage;
    - Removable or external hard drive storage;
    - CD/DVD disks;
    - Smartcards;
- Time-sensitive data;
- Access control devices and systems;
- Biometric systems and devices;
- Boundary protection devices and systems;
- Databases;
- Detection devices and systems;
- ICs, smart cards and smart card-related devices and systems;
- Key management systems;
- Multi-function devices;
- Network and network-related devices and systems;
- Operating systems;
- Products for digital signatures;
- Trusted computing.

Security strengths, algorithms and protocols:

Approved algorithms and associated security strengths can be found in ISO/IEC 19790:2012, Annexes C and D.

The organization should also consider the interoperability of various cryptographic modules as the API's provided may not be compatible between products or vendors.

Once all data that requires cryptographic protection is identified, where cryptographic security needs to be implemented, selection of security algorithms, strength and protocols and interoperability addressed, the organization should develop security policies that reflect these decisions. The security policies should address both where data is to be protected, and when the same data does not need protection.

10.3 Cryptographic module assurance

Once a policy has identified that data is to be protected in 10.2, the organization starts the search for an appropriate cryptographic module. A user should limit their selection of a cryptographic module to one that has been validated by a validation authority to ISO/IEC 19790. This validation provides a baseline level of assurance of the attributes of the cryptographic module. Typically, a validation authority provides public lists of those modules have been validated by that validation authority (e.g. Annex A). An organization can determine which lists to use for a module selection. For example, a government entity can have a list that is a subset of a validation authorities listing.

10.4 Interoperability

As referenced in 10.2, many cryptographic modules can implement the same algorithms with appropriate security strengths, but the APIs provided by each of those cryptographic modules can be incompatible. This issue is often apparent between different vendors, but can occur even within a vendor's own products. In addition to the APIs, the protocols used for key management and the interoperability with key management systems need to be considered.

10.5 Selection of security rating for SSP protection

As referenced in Clause 9, the physical and operational environment needs to be considered to determine the overall security rating or individual security rating to be selected. Depending on the security rating selected, the module's protection of SSPs can be provided by the physical environment (e.g. within an access controlled facility) or by the module itself. For each module deployed by the organization, the physical environment needs to be considered based on the value or sensitivity of the data or SSPs that the module processes.

11 Principles for operational testing

11.1 General

This clause describes the principles for operational testing that assesses the installation, configuration, operation and key management and security requirements of authentication credential in the operational environment to give confidence that the cryptographic module functions correctly and securely, that vulnerabilities have been properly considered, and verifies that the information provided in the security policy document in compliance with ISO/IEC 19790 is correct.

Cryptographic modules and their operational environments are generally complex. When cryptographic modules are deployed in their operational environment, even a minor error or mistake in configuration or initialisation can affect the security of the whole security system. So, it is important to perform operational testing, and it is necessary to select a proper cryptographic module in the operational environment throughout the operational testing.

During the operation of cryptographic modules, it should be considered that the users of the cryptographic module can be less trustworthy, less experienced, less competent and/or less motivated than that assumed during the validation. Operational testing for the cryptographic modules should be performed once the modules are integrated into their operational environments and before operation of cryptographic modules begins.

For security assurance, the organization should test the validated cryptographic module in their operational or application environment to assess whether the module operates properly as installed and configured (as specified in the security policy) and interoperates with the security system which it is deployed in.

The security system's owner should specify the security requirements to protect assets (data to need cryptographic protection) after considering the budget, the organizational security policy, value of assets, the threats, the vulnerabilities, etc.

When a cryptographic module is utilized in a diversity of application environments, operational testing should be performed to confirm that the cryptographic module can be properly utilized in each of the application environments.

In the case of ISO/IEC 19790, the validation for the cryptographic modules takes place when their development is complete and before the cryptographic module is put into operation in its environment.

The operational testing should take place before the module is put into operation. Operational testing can also be repeated after the organization has granted the authority to operate, depending on the organization's policy.

The operational testing process, as shown in Figure 5, is performed to select a proper cryptographic module for use in a specific one among a diversity of operational environments. The result of the operational testing process can be used as an input to the organization's accreditation of the cryptographic module.

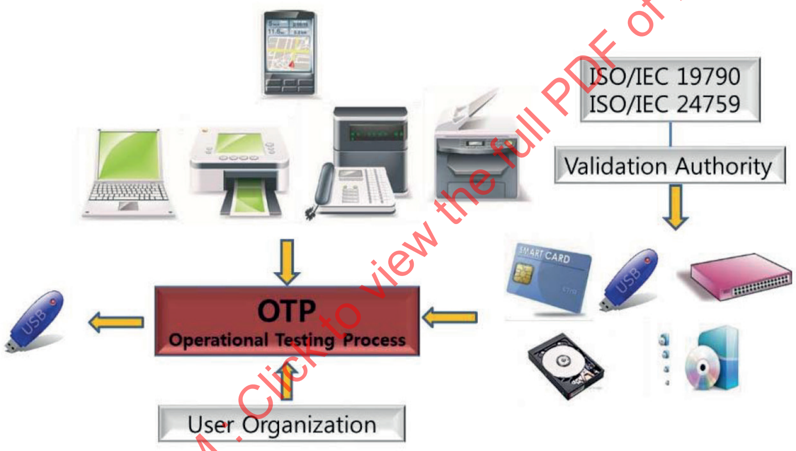

Figure 5 — Operational testing process

11.2 Assumptions

This document assumes that the security requirements related to the cryptographic modules which are required in their operational environment are provided by the organization. If the security requirements are not ready or not provided, the tester cannot proceed with the operational testing.

This document assumes that there are cryptographic modules which satisfy the security requirements of ISO/IEC 19790 have been validated by a validation authority. Typically, the validation authority provides public lists of those modules have been validated by the validation authority.

11.3 Operational testing activities

The tester should perform the operational testing in the organization's operational environment to inspect that the cryptographic modules satisfy the specified security requirements for the operational environment.

A minimum set of activities for the operational tester to follow during operational testing are as follows:

a) planning the operational testing which should include:

   1) the time that the operational testing will occur;

   2) operational testing-related documents which will be prepared;

   3) resources which the operational testing test will require, including manpower, test equipment, and time needed to complete the testing;

   4) evidences which can be gained from other tests, etc.; and

   5) the necessary tools and testing environment needed to be used;

b) producing testing evidence from the operational testing;

c) evaluating the evidence to produce the results of the operational testing;

d) reporting.

11.4 Competence for operational testers

The organization should determine the competence requirements for operational testers.

To support the goal which is to select proper cryptographic modules in the operational environment, it is necessary for testers to have gained the minimum necessary knowledge, skills, experience and qualifications relevant to ISO/IEC 19790 and ISO/IEC 24759.

Additional elements of competence such as aptitude, enthusiasm, initiative, leadership, teamwork and willingness can be required by the organization.

11.5 Use of validated evidence

For validated cryptographic modules, there can be evidence available from the module validation that can be reused in operational testing. However, the detailed evidence is not necessarily publicly available. In some instances, detailed evidence can be obtained directly from the vendor.

If the detailed evidence necessary to determine its applicability to an operational environment is not available, then the tester should determine whether it is acceptable to accept the published non-detailed evidence.

The vendor can also provide other documentation that is not referenced by the validation's security policy. Therefore, the vendor can be asked to provide the additional documentation or to create new supplemental documentation.

11.6 Documentation

There are minimum documentation requirements for operational testing which describes the cryptographic module and the operational environment which should be provided by the vendor, the validation authority and the organization:

— guidance documents describing installation, configuration and operation of the cryptographic module;

— Security Policy document in compliance with ISO/IEC 19790; and

— the organization's documentation specifying the security functions for cryptographic modules and the security requirements for the operational environment.

11.7 Operational testing procedure

The operational testing procedure consists of six steps:

a) Step 1: Planning for the operational testing;

b) Step 2: Preparing documents;

c) Step 3: Preparing configuration and testing equipment;

d) Step 4: Performing operational testing;

e) Step 5: Evaluation of the results; and

f) Step 6: Reporting the results.

12 Recommendations for operational testing

12.1 General

The organization should perform operational testing for cryptographic modules in their operational environment to determine that they satisfy the security requirements related to them for the operational environment.

The organization searches for a cryptographic module which satisfies the use policy and security requirements for their operational environment. An organization should limit their selection of a cryptographic module to one that has been validated by a validation authority to ISO/IEC 19790. This validation provides a baseline level of assurance of the attributes of the cryptographic module. Typically, a validation authority provides public lists of those modules have been validated by that validation authority. An organization should determine which validation lists are approved to use for cryptographic module selection.

After the organization selects cryptographic modules according the method specified in Clause 10, such that the security requirements for the cryptographic modules specified in Clause 7 satisfy the security requirements for the operational environment specified in Clause 9, the organization performs operational testing with the selected cryptographic modules.

The tester can use the evidences of the pre-operational test (based on the validation) to shorten the period of operational testing if the operational environment and the pre-operational environment are the same.

NOTE Annex B provides an example of a checklist that consolidates the lists given in this document.

12.2 Recommendations for assessing the installation, configuration, and operation of the cryptographic module

12.2.1 General

This subclause provides recommendations for assessing that the cryptographic modules, or their integration, is installed, configured, started up, operated, and interoperates securely and correctly by using results from pre-operational testing. Also, it provides recommendations for confirming that the cryptographic modules, or their integration, interoperate securely and correctly within the security system. (e.g. key management system as like PKI).

The operational tester should assess whether the components and interfaces that comprise the cryptographic modules, can be installed, configured in their operational environment according to the supporting documents including installation, configuration and operation procedures.

12.2.2 Assessing installation of the cryptographic module

This subclause provides recommendations for operational testers on how to assess that modules are installed securely and correctly in their specified operational environment.

Security requirements for installation of cryptographic modules are referenced in ISO/IEC 19790:2012, 7.11.7.

The operational tester should collect the evidence which is necessary for verification of secure installation, start-up and interoperation of the cryptographic modules in their operational environment.

Examples of the evidence:

- documents which specify the procedures for installation in operational environment;
- installing or reinstalling the cryptographic module based on the administrator manual;
- results from self-test (e.g. software/firmware integrity test, etc.) of the cryptographic module in its operational environment;
- results from checking tamper evidences for hardware module;
- log files; and
- fault injection files, attacks scenarios.

During the installation, the technical and operational controls can be implemented and prepared for the use of cryptographic modules in their operational environment. There can be site-specific controls and other controls which should be tested as parts of operational testing to ensure that they perform correctly in the operational environment.

For the purposes of correctness, the controls should be compliant with the security requirements for the cryptographic modules and their operational environment and authorized for the use by a competent administrator.

NOTE Refer to ISO/IEC 27001 for examples of controls for the operational environment.

Examples of technical controls:

- managing the configuration for the cryptographic modules;
- SSP generation outside of the cryptographic module;
- SSP update and access outside of the cryptographic module;
- creating a file for integration of the cryptographic modules; and
- collecting Entropy source from outside of the cryptographic module.

Examples of operational controls:

- reporting the current configuration; and
- behaviour in case of errors, alarms, default modes.

The tester should ensure that all installations can be repeated and be deleted correctly in the operational environment.

12.2.3 Assessing the configuration of the cryptographic module

Cryptographic module configuration is generally initially performed during installation. The operational tester should assess that the secure installation procedures result in a secure configuration.

There are two types of configuration:

1) the configuration of the cryptographic modules to provide the security services to enable secure for the mission that the operational environment supports; and

2) the configuration of the operational subsystem to interoperate as components of the operational environment.

The tester compares the actual configuration with the intended configuration and should ensure that the module is configured correctly and securely in the operational environment.

This guideline describes an assessment that modules are configured in the operational environment in a way that satisfies the security which the operational environment requires.

The following list gives configuration requirements typically related to cryptographic modules.

- Use of approved security services: ISO/IEC 24759 does not address testing of non-approved security services, but testing of approved security services. If the organization utilizes non-approved security services, the operational environment may create a risk to operational security.
- Use of approved security function algorithms and strengths.
- Operational security functions and non-operational security functions (e.g. degraded operation).
- SSP, CSP, PSP configuration. Key usage and key separation determined.
- SSP (Key, password, authenticate data, etc.) set by default value.
- Audit data writing, access, or storage configuration.
- Tamper configuration, if applicable.
- Operational environment configuration (access control, off-line, on-line, etc.).
- Use of validated cryptographic modules

In assessing the cryptographic module's configuration, the operational tester should:

- be sure that the cryptographic module is the validated version; and
- know what should be incorporated into the validated module.

Operational testers should determine if the crypto officer (the administrator of the cryptographic module) knows and understands as a minimum:

a) the impacts of updating, removing or inserting of the cryptographic modules;

b) the configuration of the cryptographic module and the operational environment related to it.

Also, the operational tester should collect the evidence for verification of secure configuration.

Examples of the evidence:

- records of installation and modification against actual system status;
- independently rebuilding the system; and
- checking for consistency.

The tester should ensure that all the configuration procedures can be repeated in operational environment.

12.2.4 Assessing the correct operation of the cryptographic module

This describes the assessment that modules are operated in their operational environment to satisfy the security requirements specified for the operational environment. The operational tester should use test data (sample data) instead of real data while inspecting operation.

The operational tester should assess that normal functions including installation and configuration operate securely and correctly (e.g. bypass mode).

The followings are operation test items related to the cryptographic module and should be assessed:

- entry input sample values to module in the operational environment. The set of the input sample values should be determined to be proper for the purpose of the operational testing (e.g. use case of the cryptographic module);
- approved security functions or non-approved security functions are performed as expected during the operation of the cryptographic module;
- validated cryptographic modules or non-validated cryptographic modules utilized as expected in operational environment;
- correct interoperability of module with key management system (e.g. PKI);
- correct interoperability of module with other security systems and devices;
- unauthorized operation for the cryptographic module have not occurred; and
- the cryptographic modules are performing their functions securely during operation.

12.3 Recommendations for inspecting a key management system

This subclause provides recommendations for inspecting the security requirements for a key management system and inspecting that the cryptographic modules satisfy the security requirements for it.

The operational tester should inspect security policies for key management system, type of SSPs managed in key management system, and interfaces in which key management system and cryptographic module interoperate.

Examples of the security policies for key management system:

- key size, key generation, key protection (storage, zeroization, recovery);
- the approved security functions;
- the distributing method for SSPs;
- the agreement method for SSPs; and
- the authenticating method for public key.

The tester should inspect security functions which utilize SSPs in key management system.

Examples of the security functions in key management system:

- the approved and non-approved security functions in key management system;
- security functions and interfaces which key management system and cryptographic module interoperate;
- SSP generation in key management system;
- SSP establishment in key management system;
- PSP authentication in key management system;

- SSP revocation in key management system;
- SSP destruction in key management system (e.g. zeroization); and
- the RBG entropy source; whether the entropy source is imported from key management system into cryptographic module or exported from cryptographic module.

The tester should inspect security functions which utilize SSPs in cryptographic module.

Examples of the functions in cryptographic module:

- SSP generation;
- SSP establishment:
  - automated SSP transport or SSP agreement;
  - manual SSP entry or output via direct or electronic;
- SSP entry and output;
- SSP storage; and
- SSP zeroization.

The operational tester should ensure that the interfaces for SSP entry and output between cryptographic module and key management system are correct.

The operational tester should ensure that the interoperability between the key management system and the cryptographic module about SSPs is correct.

12.4 Recommendations for inspecting the security requirements of authentication credentials

This subclause provides recommendations to support inspection that cryptographic modules satisfy the security requirements specified for authentication credentials.

The operational tester should inspect authentication credentials which are used in the operational environment and the method to protect against the authentication credentials.

Examples of the authentication credentials:

- public key/private key pair;
- certificate issued by certification authority;
- information related to certification authority;
- passwords; and
- personal authentication information.

If the cryptographic module issues the authentication credentials or is used to protect the authentication credentials, then the cryptographic module should satisfy any security requirements itself.

Examples of security requirements for the authentication credentials:

- public key/private key pair: The user's private key should be protected and should be stored securely according to security level of cryptographic module. Users should use the public key after it has been authenticated;, and
- storage, default, key erasure, recovery, number of attempts authorized.