TECHNICAL SPECIFICATION

ISO/IEC TS 23532-2

First edition
2021-11

Information security, cybersecurity and privacy protection — Requirements for the competence of IT security testing and evaluation laboratories —

Part 2: Testing for ISO/IEC 19790

Sécurité de l'information, cybersécurité et protection de la vie privée — Exigences relatives aux compétences des laboratoires d'essais et d'évaluation de la sécurité TI —

Partie 2: Essais pour l'ISO/IEC 19790

Reference number
ISO/IEC TS 23532-2:2021(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
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.

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 or www.iec.ch/members_experts/refdocs).

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) or the IEC list of patent declarations received (see https://patents.iec.ch).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of 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 www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

A list of all parts in the ISO/IEC 23532 series can be found on the ISO and IEC websites.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

Introduction

Laboratories performing testing for conformance to ISO/IEC 19790 and the test requirements in ISO/IEC 24759 may utilize and require conformance to ISO/IEC 17025:2017. ISO/IEC 17025:2017 gives generalized requirements for a broad range of testing and calibration laboratories to enable them to demonstrate that they operate competently and are able to generate valid results.

Laboratories that perform such validations have specific requirements for competence to ISO/IEC 19790 that will enable them to generate valid results.

By providing additional details and supplementary requirements to ISO/IEC 17025:2017 that are specific to information security testing and evaluation laboratories, this document will facilitate cooperation and better conformity and harmonization between laboratories and other bodies. This document may be used by countries and accreditation bodies as a set of requirements for lab assessments and accreditations.

To help implementers, this document is numbered identically to ISO/IEC 17025:2017. Supplementary requirements are presented as subclauses additional to ISO/IEC 17025:2017.

Information security, cybersecurity and privacy protection — Requirements for the competence of IT security testing and evaluation laboratories —

Part 2: Testing for ISO/IEC 19790

1 Scope

This document complements and supplements the procedures and general requirements found in ISO/IEC 17025:2017 for laboratories performing testing based on ISO/IEC 19790 and ISO/IEC 24759.

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 17000, *Conformity assessment — Vocabulary and general principles*

ISO/IEC 17025:2017, *General requirements for the competence of testing and calibration laboratories*

ISO/IEC 19790, *Information technology — Security techniques — Security requirements for cryptographic modules*

ISO/IEC 19896-1, *IT security techniques — Competence requirements for information security testers and evaluators — Part 1: Introduction, concepts and general requirements*

ISO/IEC 19896-2, *IT security techniques — Competence requirements for information security testers and evaluators — Part 2: Knowledge, skills and effectiveness requirements for ISO/IEC 19790 testers*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in in ISO/IEC 17000, ISO/IEC 17025:2017, ISO/IEC 19790, ISO/IEC 19896-1, ISO/IEC 19896-2 and the following apply.

ISO and IEC maintain terminology 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
cryptographic security testing laboratory
testing laboratory
laboratory performing cryptographic module security testing and/or cryptographic algorithms conformance testing

Note 1 to entry: See ISO/IEC 24759 for cryptographic module security testing.

Note 2 to entry: See ISO/IEC 18367 for cryptographic algorithms conformance testing.

3.2
implementation under test
IUT
implementation which is tested based on methods specified in this document

[SOURCE: ISO/IEC 17825:2016, 3.9, modified — "International Standard" changed to "document".]

4 General Requirements

4.1 Impartiality

4.1.1 ISO/IEC 17025:2017, 4.1.1 applies.

4.1.1.1 ISO/IEC 17025:2017, 4.1.1 applies with the following additions.

The laboratory shall establish and maintain policies and procedures for maintaining laboratory impartiality and integrity in the conduct of cryptographic testing. To avoid any conflict of interest, laboratory policies and procedures shall ensure that the laboratory cannot perform conformance testing if it is currently providing, or has previously provided consulting services, to the vendor for the implementation under test (IUT) (e.g. develop testing evidence, design advice).

NOTE A laboratory can provide clarification of the standards, the test requirements, and other associated documents at any time during the life cycle of the IUT which is not deemed a conflict of interest.

4.1.2 ISO/IEC 17025:2017, 4.1.2 applies.

4.1.2.1 ISO/IEC 17025:2017, 4.1.2 applies with the following additions.

The laboratory shall have no financial interest for the work performed other than its conformance testing and/or validation fees.

4.1.3 ISO/IEC 17025:2017, 4.1.3 applies.

4.1.3.1 ISO/IEC 17025:2017, 4.1.3 applies with the following additions.

The laboratory shall not perform conformance testing on a module for which the laboratory has:

a) designed any part of the IUT;

b) developed original documentation for any part of the IUT;

c) built, coded or implemented any part of the IUT;

d) had any ownership or vested interest in the IUT; or

e) provided consulting for any part of the IUT.

NOTE The laboratory can perform conformance testing on an IUT produced by a company when:

— the laboratory has no ownership in the company;

— the laboratory has a separate management from the company; and

— business between the cryptographic security testing laboratory and the company is performed under contractual agreements, as done with other clients.

4.1.4 ISO/IEC 17025:2017, 4.1.4 applies.

4.1.4.1 ISO/IEC 17025:2017, 4.1.4 applies with the following additions.

A laboratory may take existing vendor documentation for an IUT (post-design and post-development) and consolidate or reformat the information (from multiple sources) into a set format.

4.1.5 ISO/IEC 17025:2017, 4.1.5 applies.

4.2 Confidentiality

4.2.1 ISO/IEC 17025:2017, 4.2.1 applies.

4.2.2 ISO/IEC 17025:2017, 4.2.2 applies.

4.2.3 ISO/IEC 17025:2017, 4.2.3 applies.

4.2.4 ISO/IEC 17025:2017, 4.2.4 applies.

5 Structural requirements

5.1 ISO/IEC 17025:2017, 5.1 applies.

5.1.1 ISO/IEC 17025:2017, 5.1 applies with the following additions.

Laboratories shall ensure separation between laboratory testers and the company's resources who may have an interest in or may influence testing outcome.

5.1.2 ISO/IEC 17025:2017, 5.1 applies with the following additions.

For any other services of the laboratory's parent corporation not listed in 5.1, the laboratory shall have an explicit policy and a set of procedures for maintaining a strict separation, both physical and electronic, between the laboratory testers and company's consultant teams, product developers, system integrators, and others who may have an interest in and/or may unduly influence the testing outcome.

5.2 ISO/IEC 17025:2017, 5.2 applies.

5.3 ISO/IEC 17025:2017, 5.3 applies.

5.3.1 ISO/IEC 17025:2017, 5.3 applies with the following additions.

The laboratory shall define and state the scope of laboratory activities including the following:

a) selected standard(s);

EXAMPLE 1 Such as ISO/IEC 19790 and ISO/IEC 24759 which address cryptographic module requirements and testing.

1) security level(s) and area(s);

EXAMPLE 2 Such as up to overall security rating 2 and physical security level 3.

2) physical embodiment(s);

EXAMPLE 3 Such as multi-chip embedded cryptographic modules and multi-chip standalone cryptographic modules.

3) type(s) of cryptographic modules;

EXAMPLE 4 Such as a software (cryptographic) module.

b) laboratory's permanent facility.

5.3.2 ISO/IEC 17025:2017, 5.3 applies with the following optional additions.

The laboratory should define and state the scope of laboratory activities including the following:

a) categories of cryptographic algorithms and protocols which the laboratory is competent to test;

EXAMPLE 1 Such as symmetric key cryptographic algorithms and dedicated hash functions.

EXAMPLE 2 Such as various cryptographic algorithms employed in Transport Layer Security (TLS) protocol.

b) product technology types which the laboratory is competent to test.

EXAMPLE 3 Such as USB flash drives.

EXAMPLE 4 Such as Self-Encrypting Drives with SATA interface.

EXAMPLE 5 Such as network encryption devices with IPsec protocol.

5.4 ISO/IEC 17025:2017, 5.4 applies.

5.5 ISO/IEC 17025:2017, 5.5 applies.

5.6 ISO/IEC 17025:2017, 5.6 applies.

5.7 ISO/IEC 17025:2017, 5.7 applies.

6 Resource requirements

6.1 General

ISO/IEC 17025:2017, 6.1 applies.

6.1.1 ISO/IEC 17025:2017, 6.1 applies with the following additions.

The management system documentation shall contain all documentation that describes and details the laboratory's implementation of procedures covering all the technical requirements in ISO/IEC 17025:2017 and this document.

6.2 Personnel

6.2.1 ISO/IEC 17025:2017, 6.2.1 applies.

6.2.1.1 ISO/IEC 17025:2017, 6.2.1 applies with the following additions.

The laboratory shall maintain responsible supervisory personnel and competent technical staff that are:

a) knowledgeable of all scheme-specific test methods, test metrics and implementation guidance;

b) knowledgeable of all relevant international standards, and references in this document;

c) familiar with cryptographic terminology and families of cryptographic algorithms and security functions; and

d) familiar with the cryptographic testing tools.

6.2.1.2 ISO/IEC 17025:2017, 6.2.1 applies with the following additions.

The laboratory shall continuously maintain competent testers.

NOTE See ISO/IEC 19896-2 for a definition of areas that constitute required proficiency.

6.2.2 ISO/IEC 17025:2017, 6.2.2 applies.

NOTE 1 The "technical knowledge" in ISO/IEC 17025:2017, 6.2.2 is described in ISO/IEC 19896-2:2018, Clause 6.

NOTE 2 The "skills" in ISO/IEC 17025:2017, 6.2.2 are described in ISO/IEC 19896-2:2018, Clause 7.

6.2.2.1 ISO/IEC 17025:2017, 6.2.2 applies with the following additions.

The laboratory shall maintain a list of the key personnel, including their assigned roles and a summary of their latest training qualifications. The list shall include, but shall not be limited to:

a) laboratory director;

b) laboratory manager(s);

c) staff members(s) responsible for maintaining management system;

d) authorized representative;

e) approved signatories; and

f) other key technical persons in the laboratory (e.g. testers).

NOTE 1 Significant change in a laboratory's key technical personnel or facilities can result in a laboratory no longer being deemed proficient by relevant scheme owner(s).

NOTE 2 In order to perform objective and meaningful reviews of reported results in ISO/IEC 17025:2017, 7.7.1, item i), the laboratory can employ multiple testers to ensure that another qualified and competent tester is in charge of the review, who is not involved in testing the IUT subject to review.

6.2.2.2 ISO/IEC 17025:2017, 6.2.2 applies with the following additions.

Laboratories shall document the required qualifications for each staff position.

NOTE Staff information can be kept in the official personnel folders.

6.2.2.3 ISO/IEC 17025:2017, 6.2.2 applies with the following additions.

The number of qualified testers within the laboratory shall be greater than or equal to the scheme-specific minimum required number of testers.

EXAMPLE Such as a minimum of two qualified testers.

6.2.3 ISO/IEC 17025:2017, 6.2.3 applies.

6.2.3.1 ISO/IEC 17025:2017, 6.2.3 applies with the following additions.

If the mechanism by which the laboratory employs staff members is through contracting of personnel, any key personnel who are contractors shall be identified and listed.

6.2.4 ISO/IEC 17025:2017, 6.2.4 applies.

6.2.4.1 ISO/IEC 17025:2017, 6.2.4 applies with the following additions.

An individual may be assigned or appointed to serve in more than one position provided it does not create a conflict of interest and maintains impartiality. To the extent possible, the laboratory director and the person responsible for implementing and maintaining the management system should be independently staffed.

6.2.5 ISO/IEC 17025:2017, 6.2.5 applies.

6.2.5.1 ISO/IEC 17025:2017, 6.2.5 applies with the following additions.

The laboratory person(s) responsible for implementing and maintaining the management system shall receive management system training preferably in ISO/IEC 17025:2017. If training is not available in ISO/IEC 17025:2017, minimum training shall be acquired in the ISO 9000 family of standards, especially ISO 9001, or equivalent with emphasis for internal auditing.

6.2.5.2 ISO/IEC 17025:2017, 6.2.5 applies with the following additions.

The laboratory shall have a competency review program and procedures for the evaluation and maintenance of the competency of each staff member for each test method the staff member is authorized to conduct. An evaluation and an observation of performance shall be conducted annually for each staff member by the immediate supervisor or a designee appointed by the laboratory director. A record of the annual evaluation of each staff member shall be dated and signed by the supervisor and the employee.

6.2.5.3 ISO/IEC 17025:2017, 6.2.5 applies with the following additions.

The laboratory management shall ensure adequate training for the laboratory staff as directed in 6.2.5.1. The personnel shall possess knowledge of or be trained in ISO/IEC 19896-2.

6.2.6 ISO/IEC 17025:2017, 6.2.6 applies.

6.3 Facilities and environmental conditions

6.3.1 ISO/IEC 17025:2017, 6.3.1 applies.

6.3.1.1 ISO/IEC 17025:2017, 6.3.1 applies with the following additions.

The laboratory shall have its internal networks protected from unauthorized access by external entities, as well as protection against malicious software.

6.3.1.2 ISO/IEC 17025:2017, 6.3.1 applies with the following additions.

Within the internal networks, information/data shall be protected commensurate with their classification and/or sensitivity, and access to them shall be given only to authorized personnel.

6.3.1.3 ISO/IEC 17025:2017, 6.3.1 applies with the following additions.

NOTE In considering a test setup of an IUT, the test harness and supporting/surrounding test apparatus can impose constraints such as performance and availability. Such equipment is appropriately selected.

EXAMPLE Network throughput may affect the determination of pass/fail of assertion [04.50] (the strength of the authentication objective), because the number of authentication requests can be limited by the network throughput.