SLOVENSKI STANDARD
oSIST prEN ISO/IEC 19896-2:2025

01-januar-2025

Informacijska varnost, kibernetska varnost in varovanje zasebnosti - Zahteve za usposobljenost osebja za ugotavljanje skladnosti z varnostjo IT- 2. del: Zahteve glede znanja in spretnosti za preizkuševalce in potrjevalce ISO/IEC 19790 (ISO/IEC DIS 19896-2:2024)

Information security, cybersecurity and privacy protection - Requirements for the competence of IT security conformance assessment body personnel - Part 2: Knowledge and skills requirements for ISO/IEC 19790 testers and validators (ISO/IEC DIS 19896-2:2024)

Sécurité de l'information, cybersécurité et protection de la vie privée - Exigences relatives aux compétences du personnel des organismes d'évaluation de la conformité de la sécurité TI - Partie 2: Exigences en matière de connaissances et de compétences pour les testeurs de l'ISO/IEC 19790 (ISO/IEC DIS 19896-2:2024)

Ta slovenski standard je istoveten z: **prEN ISO/IEC 19896-2**

ICS:

03.100.30	Vodenje ljudi	Management of human resources
35.030	Informacijska varnost	IT Security

oSIST prEN ISO/IEC 19896-2:2025 **en,fr,de**

DRAFT International Standard

ISO/IEC DIS 19896-2

Information security, cybersecurity and privacy protection — Requirements for the competence of IT security conformance assessment body personnel —

Part 2: Knowledge and skills requirements for ISO/IEC 19790 testers and validators

ICS: 35.030

ISO/IEC JTC **1**/SC **27**

Secretariat: **DIN**

Voting begins on:
2024-11-11

Voting terminates on:
2025-02-03

This document is circulated as received from the committee secretariat.

ISO/CEN PARALLEL PROCESSING

Reference number
ISO/IEC DIS 19896-2:2024(en)

COPYRIGHT PROTECTED DOCUMENT

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 ..... **iv**
Introduction ..... **v**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **1**
4 Abbreviated terms **2**
5 Structure of this document **2**
6 Knowledge **2**
6.1 General 2
6.2 Testers 2
6.2.1 Tertiary education 2
6.2.2 Knowledge of standards 7
6.2.3 Knowledge of the validation program 8
6.2.4 Knowledge of the requirements of ISO/IEC 23532-2 9
6.3 Validators 10
6.3.1 Tertiary education 10
6.3.2 Knowledge of standard 10
6.3.3 Knowledge of the validation program 10
6.3.4 Knowledge of the requirements of ISO/IEC 23532-2 and validation authority 11
7 Skills **12**
7.1 Testers 12
7.1.1 General 12
7.1.2 Algorithm testing 12
7.1.3 Physical security testing 12
7.1.4 Side channel analysis 12
7.1.5 Technology types 12
7.2 Validators 12
Annex A (informative) **Example of an ISO/IEC 24759 testers' and validators' log** **13**
Annex B (informative) **Ontology of technology types** **14**
Annex C (informative) **Specific knowledge associated with the security of cryptographic modules being tested for conformity to ISO/IEC 19790:2012** **17**
Bibliography **34**

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 documents 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 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.

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

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.

A list of all parts in the ISO/IEC 19896 series can be found on the ISO website.

This second edition cancels and replaces the first edition (ISO/IEC 19896-2), which has been technically revised. The main changes compared to the previous edition are the following:

- The document has been restructured
  - Delete subclauses related to experience, education and effectiveness
- Technical changes have been introduced
  - Rewrite knowledge and skill as the remaining part of the elements of competence; knowledge, skills, experience, education and effectiveness according to CASCO's comments
  - Add competence requirements for the validators
  - Update Annex C to be aligned with ISO/IEC 19790 and to avoid duplication

Introduction

This document provides the specialized requirements to demonstrate knowledge and skills requirements of individuals in performing security testing projects in accordance with ISO/IEC 19790 and ISO/IEC 24759. ISO/IEC 19790 provides the specification of security requirements for cryptographic modules. Many validation schemes and recognition arrangements have been developed using it as a basis. ISO/IEC 19790 permits comparability between the results of independent security testing projects. ISO/IEC 24759 supports this by providing a common set of testing requirements for testing a cryptographic module for conformance with ISO/IEC 19790.

One of important factors in assuring comparability of the results of such validations is the knowledge and skills requirements of the individual testers responsible for performing testing projects.

Other factor in assuring comparability of the results of such validations is the knowledge and skills requirements of the individual validators responsible for performing validating projects.

ISO/IEC 23532-2, which is often specified as a standard to which the testing laboratory shall ensure, states in 6.2 that the competence requirements for each function influencing the results of laboratory activities, including requirements for education, qualification, training, technical knowledge, skills and experience are documented and the personnel have the competence to perform laboratory activities for which they are responsible and to evaluate the significance of deviations.

The audience for this document includes validation authorities, accreditation bodies for testing laboratory or validation authority, testing laboratories, testers, validators and organizations offering professional credentials and recognitions.

This document establishes a baseline for the knowledge and skills requirements of ISO/IEC 19790 testers with the goal of establishing conformity in the requirements for the training of ISO/IEC 19790 testing professionals associated with cryptographic module conformance testing programs and ISO/IEC 19790 validators with the goal of establishing conformity in the requirements of ISO/IEC 19790 validating professionals associated with cryptographic module validation program.

Information security, cybersecurity and privacy protection — Requirements for the competence of IT security conformance assessment body personnel —

Part 2: Knowledge and skills requirements for ISO/IEC 19790 testers and validators

1 Scope

This document provides the minimum requirements for the knowledge and skills requirements of assessment body personnel performing testing activities and validating activities for a conformance scheme using 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 17825, *Information technology — Security techniques — Testing methods for the mitigation of non-invasive attack classes against cryptographic modules*

ISO/IEC 18367, *Information technology — Security techniques — Cryptographic algorithms and security mechanisms conformance testing*

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 20085-1, *IT Security techniques — Test tool requirements and test tool calibration methods for use in testing non-invasive attack mitigation techniques in cryptographic modules — Part 1: Test tools and techniques*

ISO/IEC 20085-2, *IT Security techniques — Test tool requirements and test tool calibration methods for use in testing non-invasive attack mitigation techniques in cryptographic modules — Part 2: Test calibration methods and apparatus*

ISO/IEC 20543, *Information technology — Security techniques — Test and analysis methods for random bit generators within ISO/IEC 19790 and ISO/IEC 15408*

ISO/IEC 23532-2, *Information security, cybersecurity and privacy protection — Requirements for the competence of IT security testing and evaluation laboratories — Part 2: Testing for ISO/IEC 19790*

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

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 19896-1, ISO/IEC 23532-2 and ISO/IEC 19790 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/

4 Abbreviated terms

AES advanced encryption standard

HDD hard disk drive

RSA rivest-shamir-adleman

SHA secure hash algorithm

SSD solid state drive

5 Structure of this document

This document is divided into the following clauses: Knowledge (Clause 5) and Skills (Clause 6). Each clause corresponds to an aspect of the knowledge and skills requirements of individuals performing testing activities or validating activities as introduced in ISO/IEC 19896-1 for a conformance scheme using ISO/IEC 19790 and ISO/IEC 24759.

6 Knowledge

6.1 General

Knowledge is what a tester or a validator knows and can describe. The difference between a validator and tester is described in more detail, plus how to use the standard for one or the other, e.g. If you are a tester, you have to comply with the following sections (6.2), and if you are a validator you have to comply with the following sections (6.3).

6.2 Testers

6.2.1 Tertiary education

6.2.1.1 General

Testers shall have educational qualifications such as an associate, bachelor, or higher degree that is relevant to the security requirements addressed in ISO/IEC 19790 and the test requirements in ISO/IEC 24759. The testers shall at a minimum demonstrate they have either:

a) successfully completed appropriate tertiary education with at least 3 years of study in disciplines related to IT or IT security; or

b) experience equivalent to the tertiary education in disciplines related to IT, IT security or IT system administration.

6.2.1.2 Technical specialties

In addition to the minimum level of educational requirements in 6.2.1.1, testers shall have educational qualifications such as an associate, bachelor, or higher degree that addresses the specific technical specialities. Examples of specific technical specialities include:

— cryptographic concepts;

— engineering technology;

— electrical engineering;

— mechanical engineering;

— material engineering;

— chemical engineering;

— computer information technology;

— computer engineering;

— computer science;

— computer networks;

— cybersecurity;

— information systems;

— laboratory management;

— mathematics and physics;

— software development and security; or

— software engineering.

6.2.1.3 Specialty topics

ISO/IEC 19790:2012 and the test requirements in ISO/IEC 24759:2017 address the following specific speciality knowledge topics. A tester shall, at a minimum, demonstrate knowledge in at least one specific speciality topic.

A testing laboratory shall have knowledge in all the speciality areas as an aggregate of its technical staff.

ISO/IEC 19790:2012 and ISO/IEC 24759:2017 specify speciality topics:

a) software and firmware development:
   1) programming languages (e.g., assembler and high-level);
   2) compilers;
   3) debugging tools;
   4) product testing performed by vendor:
      i) unit testing;
      ii) integration testing;
      iii) regression testing;

b) operating systems:
   1) installation;
   2) configuration;
   3) operation;
   4) architecture;

5) system hardening;

6) virtual machines;

7) java runtime environment;

c) hardware development:

1) hardware embodiments:

i) single-chip;

ii) multi-chip embedded;

iii) multi-chip standalone;

2) technology:

i) single-chip fabrication;

ii) electrical components and design, schematics and concepts including logic design and HDL representations;

iii) mechanical design and packaging;

3) manufacturing:

i) supply chain integrity;

ii) fabrication methods;

iii) initialization of parameters;

iv) packing and shipping;

v) testing and characterization;

4) hardware security features;

d) operational environments:

1) boot loader;

2) loading;

3) linking;

4) memory management and protection;

5) inter-process communication;

6) discretionary access control;

7) role-based access control;

8) executable forms;

9) audit mechanisms;

e) cryptographic algorithms, mechanisms and techniques:

1) cryptographic algorithms and security functions:

i) symmetric key;

ii) asymmetric key;