
**IT security techniques — Competence
requirements for information security
testers and evaluators —**

**Part 2:
Knowledge, skills and effectiveness
requirements for ISO/IEC 19790
testers**

*Techniques de sécurité IT — Exigences de compétence pour
l'information testeurs d'assurance et les évaluateurs —*

*Partie 2: Exigences en matière de connaissances, de compétences et
d'efficacité pour ISO / IEC 19790 testeurs*

ISO/IEC 19896-2:2018

<https://standards.iteh.ai/catalog/standards/iso/250748d6-e774-4625-b34d-91897b267bf8/iso-iec-19896-2-2018>



iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

ISO/IEC 19896-2:2018

<https://standards.iteh.ai/catalog/standards/iso/250748d6-e774-4625-b34d-91897b267bf8/iso-iec-19896-2-2018>



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2018

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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	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 Tertiary education	2
6.2.1 General	2
6.2.2 Technical specialities	2
6.2.3 Speciality topics	3
6.3 Knowledge of standards	7
6.3.1 General	7
6.3.2 ISO/IEC 19790 concepts	7
6.3.3 ISO/IEC 24759	7
6.3.4 Additional ISO/IEC standards	8
6.4 Knowledge of the validation program	8
6.4.1 Validation program	8
6.5 Knowledge of the requirements of ISO/IEC 17025	10
7 Skills	10
7.1 General	10
7.2 Algorithm testing	10
7.3 Physical security testing	10
7.4 Side channel analysis	10
7.5 Technology types	10
8 Experience	10
8.1 General	10
8.2 Demonstration of technical competence to the validation program	11
8.2.1 Experience with performing testing	11
8.2.2 Experience with particular technology types	11
9 Education	11
10 Effectiveness	11
Annex A (informative) Example of an ISO/IEC 24759 testers' log	12
Annex B (informative) Ontology of technology types and associated bodies of knowledge	13
Annex C (informative) Specific knowledge associated with the security of cryptographic modules	16
Annex D (informative) Competence requirements for ISO/IEC 19790 validators	33
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 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 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, *IT security techniques*.

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.

Introduction

This document provides the specialized requirements to demonstrate knowledge, skills and effectiveness 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 certification, 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 important factor in assuring comparability of the results of such validations or certifications is the knowledge, skills and effectiveness requirements of the individual testers responsible for performing testing projects.

ISO/IEC 17025, which is often specified as a standard to which testing facilities conform, states in 5.2.1 that “Personnel performing specific tasks shall be qualified on the basis of appropriate education, training, experience and/or demonstrated skills”.

The audience for this document includes validation and certification authorities, laboratory testing accreditation bodies, testing projects schemes, testing facilities, testers and organizations offering professional credentials and recognitions.

This document establishes a baseline for the knowledge, skills and effectiveness 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.

[Annex D](#) illustrates the usefulness of this document by validators within a validation program.

ITEH Standards
(<https://standards.iteh.ai>)
Document Preview

ISO/IEC 19896-2:2018

<https://standards.iteh.ai/catalog/standards/iso/250748d6-e774-4625-b34d-91897b267bf8/iso-iec-19896-2-2018>

