INTERNATIONAL STANDARD

ISO/IEC 23837-1

First edition
2023-08

Information security — Security requirements, test and evaluation methods for quantum key distribution —

Part 1: **Requirements**

Technologies de l'information — Exigences de sécurité, méthodes d'essais et d'évaluation relatives à la distribution quantique de clés —

Partie 1: Exigences

Reference number
ISO/IEC 23837-1:2023(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).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

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 23837 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

The ISO/IEC 23837 series specifies the security requirements, test and evaluation methods for quantum key distribution (QKD) under the framework of the ISO/IEC 15408 series. This document focuses on specifying the common baseline set of security functional requirements (SFRs) of QKD modules.

Theoretically, QKD provides a method to use a pre-shared key to establish a longer symmetric key with security that does not depend upon the computational power of an adversary; the established key can then be used for cryptographic purposes, such as for an encryption mechanism to create a secure communication channel.

Although the security of QKD protocols is proven through rigorous security models that assume the two communicating parties share a secret key beforehand, discrepancies between the models and practical implementations frequently occur during the life cycle phases of QKD modules. These imperfections or deviations from the security models can result in vulnerabilities that compromise the security of practical QKD systems. Among them, severe side channel attacks have been proposed and there have been some proof-of-principle demonstrations in QKD hacking experiments. Like conventional cryptographic modules or network devices, QKD modules are expected to have strict security testing and evaluation to avoid security attacks and then leakage of information before being deployed into real applications. Intensive and strict evaluation is an essential step before QKD is widely accepted by the industry.

For this purpose, the ISO/IEC 23837 series defines a set of rigorous and common security specifications for QKD modules manufacturers, so that manufacturers can follow the standard procedure to design and implement IT products that use QKD, and evaluators can follow the standard procedure to test and evaluate the security of QKD modules, reducing the risk of a failure of security in operation. This document uses the standardized model and language of the ISO/IEC 15408 series to define a common baseline set of SFRs for QKD modules. The entire implementation of QKD protocols is included, from conventional network components to quantum optical components. Annex A provides information to facilitate the development of protection profiles for QKD modules. ISO/IEC 23837-2 is intended to specify evaluation activities that are necessary for the security evaluation of QKD modules at the expected evaluation assurance levels.

NOTE In this document, the description of extended security functional components in 8.2 and SFRs in Clause 9 corresponds to the style of the description of security functional components in ISO/IEC 15408-2. This includes not only the structure of the security functional family and components, but also the font styles (i.e. bold and italics) of the text, which are described by following the convention of ISO/IEC 15408-2 to distinguish some terms from the rest of the text. In this case, users with a background in using the ISO/IEC 15408 series can easily apply the extended security functional components and the SFRs to write documents for the evaluation of QKD modules.

Information security — Security requirements, test and evaluation methods for quantum key distribution —

Part 1: Requirements

1 Scope

This document specifies a general framework for the security evaluation of quantum key distribution (QKD) according to the ISO/IEC 15408 series. Specifically, it specifies a baseline set of common security functional requirements (SFRs) for QKD modules, including SFRs on the conventional network components and the quantum optical components, and the entire implementation of QKD protocols. To facilitate the analysis of SFRs, security problems that QKD modules can face in their operational environment are analysed based on a structural analysis of the security functionality of QKD modules and the classification of QKD protocols.

The SFRs on conventional network components of QKD modules are mainly characterized under the framework of the ISO/IEC 15408 series and also refer to the methodology of ISO/IEC 19790 and relevant standards on testing of cryptographic modules and network devices.

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 15408-1:2022, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 1: Introduction and general model*

ISO/IEC 15408-2:2022, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 2: Security functional components*