INTERNATIONAL STANDARD

ISO/IEC 23837-2

First edition
2023-09

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

Part 2: Evaluation and testing methods

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

Partie 2: Méthodes d'essais et d'évaluation

Reference number
ISO/IEC 23837-2:2023(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 website.

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 security requirements, test and evaluation methods for quantum key distribution (QKD) modules under the framework of the ISO/IEC 15408 series. This document specifies an evaluation method and relevant evaluation activities for the security evaluation of QKD modules in a relatively general way. The evaluation activities that are necessary for the security evaluation of QKD modules include supplementary evaluation activities for the QKD-related security functional requirements (SFRs) specified in ISO/IEC 23837-1 and the supplementary evaluation activities for security assurance requirements (SARs) with security assurance levels ranging from evaluation assurance level (EAL) 1 to EAL 5+.

Specifically, the evaluation activities for the testing and evaluation of implementations of QKD protocols, quantum optical components in QKD transmitter modules, and QKD receiver modules are described in detail. For SFRs specific to conventional network components, this document does not specify concrete evaluation activities but mainly refers to existing methods for network devices. In addition, supplementary activities for security assurance requirements are specified, and refinements to the generic vulnerability analysis methodology in ISO/IEC 18045 are presented, including guidance on the calculation of attack potentials.

This document is expected to provide a specification to help QKD manufacturers improve the design and implementation security of QKD modules, and to guide evaluators in the testing and security evaluation of QKD modules, thus reducing the risk of failure of security in operation.

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

Part 2: Evaluation and testing methods

1 Scope

This document specifies test and evaluation methods for the security evaluation of quantum key distribution (QKD). It also describes evaluation activities that constitute the test and evaluation methods for the security functional requirements on the implementation of QKD protocols, the quantum optical components and conventional network components in QKD modules. Moreover, supplementary evaluation activities for security assurance requirements are provided to support the security evaluation of QKD with appropriate assurance levels.

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 15408-4:2022, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 4: Framework for the specification of evaluation methods and activities*

ISO/IEC 18045, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Methodology for IT security evaluation*

ISO/IEC 23837-1:2023, *Information security — Security requirements, test and evaluation methods for quantum key distribution — Part 1: Requirements*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 23837-1 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
attenuation
reduction in the intensity of a light beam relative to the distance travelled through a transmission medium

3.2
attenuator
device used to reduce the power level of a light beam

3.3
back-flash
pulse of one or more photons emitted from a single-photon detector

Note 1 to entry: This phenomenon is also known as “backflash light” or “breakdown flash”.

Note 2 to entry: This phenomenon is due to radiative charge recombination, and is observed in devices such as avalanche photodiodes where large populations of electron-hole pairs are created.

3.4
beam splitter
BS
device which can split an incident light beam at a designed ratio into two or more separate beams

3.5
correlation function
function used to characterize the statistical and coherence properties of light beams

3.6
dark count
detection event registered by an optical detector in the absence of optical illumination

3.7
dead time
time interval after a detection event when the detector as a whole is unable to provide an output in response to incoming photons at the single photon level

[SOURCE: ETSI GR QKD 007 V1.1.1:2018]

3.8
density matrix
matrix that describes the state of a quantum system

3.9
detection probability
probability that a detector registers a detection event within a stated duration time

3.10
emulator
tool with a known and trusted implementation of the expected functionality under test

3.11
fidelity
measure of the closeness of two quantum states

3.12
injected light monitor
detector for monitoring the power of the laser light injected from the quantum channel

3.13
local oscillator
LO
strong optical signal that acts as a phase reference for interference with a weak optical signal (e.g., quantum state) in coherent detection

3.14
mean photon number
average number of photons per optical pulse

[SOURCE: ETSI GR QKD 007 V1.1.1:2018]

3.15
polarization
property of electromagnetic waves that describes the orientation of the oscillating electric field vector

[SOURCE: ETSI GR QKD 007 V1.1.1:2018]

3.16
polarization analyser
instrument designed to measure and display the *polarization* (3.15) of an optical pulse

3.17
quantum state analyser
instrument designed to measure optical states in one or more specified degrees of freedom

3.18
shot noise
noise which can be modelled by a Poisson process, describing the fluctuations of the number of photons detected due to their occurrence independent of each other

3.19
spectrum analyser
instrument designed to measure and display the distribution of power of an optical source over a specified wavelength span

4 Abbreviated terms

ATE	assurance class of tests
AVA	assurance class of vulnerability assessment
cPP	collaborative PP
EA	evaluation activity
EAL	evaluation assurance level
EM	evaluation method
IT	information technology
NRBG	non-deterministic random bit generator
PP	protection profile
QKD	quantum key distribution
RX	receiver
SAR	security assurance requirement
SFR	security functional requirement
SPD	single-photon detector
TOE	target of evaluation
TSF	TOE security functionality
TSFI	TSF interface
TX	Transmitter

5 Overview of the evaluation method for QKD modules

5.1 General

The primary objective of the security evaluation of QKD modules is to validate whether the implementation of the core functionality and the IT-related security controls of QKD modules meet the security requirements of an expected evaluation assurance level (EAL).

Since the high-level generic evaluation activities (EAs) specified in ISO/IEC 18045 do not directly cover all aspects of the security evaluation of QKD modules, this document gives an evaluation method (EM) to supplement ISO/IEC 18045, by considering the characteristics of QKD modules. In particular, this EM includes some specific EAs for security functional requirements (SFRs), which are defined in ISO/IEC 23837-1, and security assurance requirements (SARs), which are defined or refined based on the work units in ISO/IEC 18045.

5.2 Scope of the evaluation method

The defined method for the security evaluation of QKD modules is based on the framework specified by ISO/IEC 15408-4. Figure 1 gives the structure of the EM based on the following considerations.

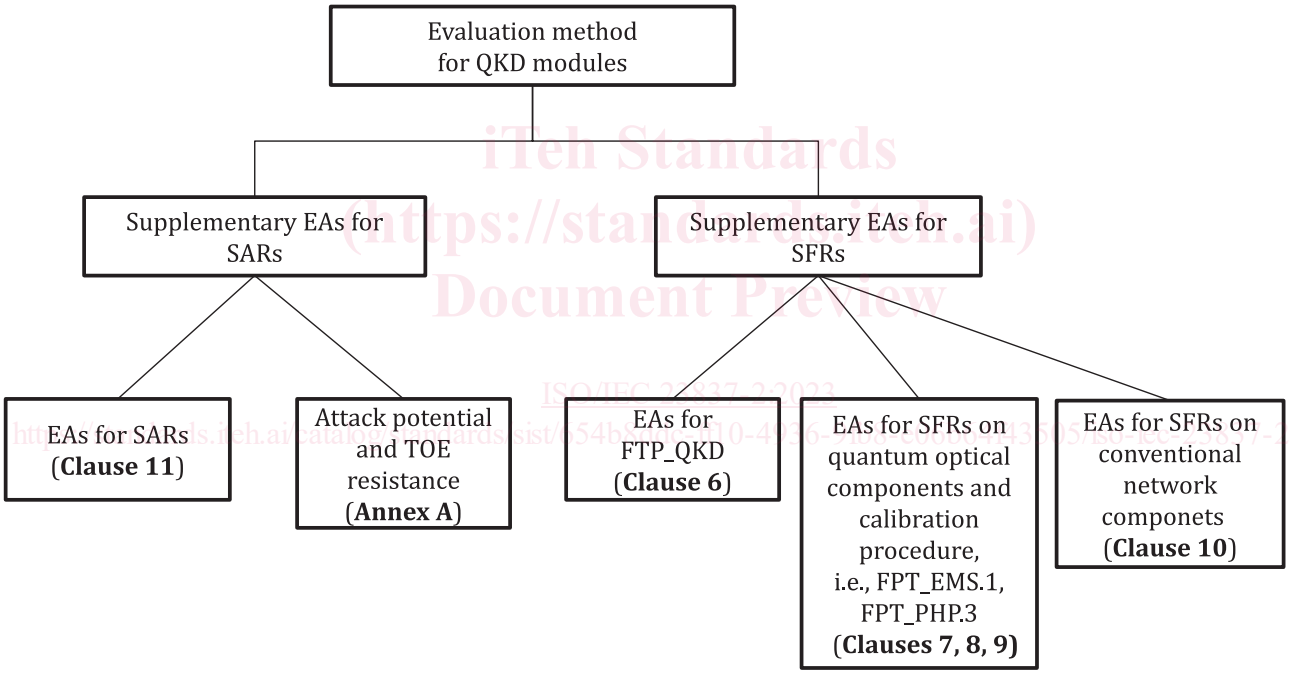

Figure 1 — Structure of the specific EM for QKD modules and its constituent EAs

The EM includes a collection of EAs for SARs and SFRs. In particular, a set of EAs for some existing SARs in ISO/IEC 18045 are supplemented to make their work units more specific for the evaluation of QKD modules, in particular those related to the assurance Class ATE and Class AVA (see 11.6, 11.7 and Annex A). In addition, a set of EAs for specific SFRs is defined, which addresses SFRs on the quantum optical components (see ISO/IEC 23837-1:2023, 9.4) and the implementation of QKD protocols (i.e. FTP_QKD). The EAs for SFRs are intended to help evaluators address evaluation actions required by the SARs ATE_IND.1 and ATE_IND.2 that are specific to QKD modules (see Clauses 6 to 9 for further detail).

On the other hand, since the objective of this document is to provide a supplementary evaluation methodology that is specific to QKD modules, EAs for common SFRs on conventional network components (including SFRs in the classes of FCS, FIA, FDP, FMT defined in ISO/IEC 15408-2) are not emphasized. As the corresponding methodology for those SFRs is relatively mature in the IT security evaluation industry, evaluators may reference existing standards or methodologies to handle

such aspects. Clause 10 explains this in more detail, and existing standards and methodologies are referenced to help evaluators select appropriate approaches.

Not all EAs in this document are required for the security evaluation of a specific TOE of QKD modules. The selection of EAs depends on the implemented QKD protocols and the implementation strategy of the TOE. Clause 12 describes the requirements of the conformance statement when a specific evaluation process claims conformance with this document.

5.3 Overview of evaluation activities for SFRs

5.3.1 General

The objective of functional testing in a security evaluation is to verify whether the implementation of the functionality and IT-related controls are consistent with the design specification, and that the security requirements defined in the ST are satisfied by the TOE. The EAs for SFRs, as specified mainly in Clauses 6, 7, 8, and 9, are intended to supplement the work units concerned with independent functional testing of the TSF, especially the work units regarding the security assurance family of ATE_IND in ISO/IEC 18045.

NOTE This includes the work units of ATE_IND.1–3, ATE_IND.1–4, ATE_IND.1–5, ATE_IND.1–6 and ATE_IND.1–7 when ATE_IND.1 is chosen for the expected EAL, or the work units of ATE_IND.2–6, ATE_IND.2–7, ATE_IND.2–8, ATE_IND.2–9 and ATE_IND.2–10 when ATE_IND.2 is chosen.

Although the EAs are intended to help evaluators of QKD modules, these EAs can also be used to help developers of QKD modules perform functional testing (for security assurance family of ATE_FUN), and ensure the evaluator that the tests have been performed and documented correctly, before applying for security evaluation/certification.

ISO/IEC 15408-4:2022, Clause 6 explains that the content generally required for the specification of an EA includes:

— objective of the evaluation activity;

— required inputs (from the developer);

— required tool types and setup;

— required evaluator competence;

— rationale (justification of their derivation from the work units in ISO/IEC 18045);

— dependencies (of the activities on other relevant EAs);

— test procedure (for performing the EA);

— pass/fail criteria (for deciding the outcome of the EA).

Regarding these EAs, the general inputs required by the evaluator (but mainly prepared by the developers) for independent testing are defined in ISO/IEC 18045, and include at least:

a) if ATE_IND.1 is concerned in the evaluation, then the following inputs are required:

— the ST;

— the functional specification;

— the guidance documentation;

— the TOE suitable for testing;

b) if ATE_IND.2 is concerned in the evaluation, then the following additional evidence is required:

— the TOE design description;

— the configuration management documentation;

— the test documentation.

In addition, all the test tools required for the EAs shall be calibrated correctly against some specific standards by default. Otherwise, the reason shall be justified in the corresponding EAs.

For each EA, it is necessary for the developer to present at least the general inputs listed in a) and b) accordingly to the evaluator. On completion of the evaluation process, the evaluator shall report the evaluation result of the EA.

The "dependencies" item specified in ISO/IEC 15408-4:2022, Clause 6 is not necessary for the description of EAs that are independent of all other EAs. The item is therefore neglected from the description of those EAs hereinafter.

5.3.2 EAs for SFRs FTP_QKD.1 and FTP_QKD.2

ISO/IEC 23837-1 defines an extended security functional family (i.e. FTP_QKD) to specify the requirements on the FUN_QKD functionality (see ISO/IEC 23837-1:2023, 6.4.2 for the definition) of QKD modules. Correspondingly, EAs related to the evaluation of the implementation of a QKD protocol, or rather the implementation of raw data generation, post-processing and parameter adjustment procedures are specified in 6.2, 6.3, and 6.4 respectively. These EAs are used to examine the correctness of the implementation of FUN_QKD (or more precisely, the SFRs FTP_QKD.1 and FTP_QKD.2).

Each of the EAs provides the required content listed in 5.3.1, especially the following:

a) Test procedures for checking the correctness of the implementation of raw data generation, post-processing and parameter adjustment procedure(s) of the TOE.

b) Pass/fail criteria (for the evaluation of an implementation of a QKD protocol).

5.3.3 EAs for SFRs on quantum optical components and parameter adjustment procedure(s)

The SFRs on quantum optical components and parameter adjustment procedure(s) mainly include FPT_EMS.1/Quantum and FPT_PHP.3 (see ISO/IEC 23837-1:2023, 9.4). These requirements are imposed on the relevant security functions that relate to quantum optical components of QKD modules and the parameter adjustment procedure(s). The expectation is that, at the expected EAL, the TOE that meets these SFRs can resist known attacks (mainly) conducted from the quantum channel.

This document describes EAs for the two SFRs representing the parts of a QKD evaluation that are most specific to QKD technology-specific evaluation activities, and are the focus of this document (see Clauses 7, 8, and 9). The common objective of these EAs is to help an evaluator examine the effectiveness of the IT-related controls used by QKD modules to resist known attacks.

Such EAs specify the required content listed in 5.3.1, especially the following:

a) Test procedures for checking the correctness of the implementation of IT-related controls employed by the QKD modules to address the identified threats to quantum optical components and the parameter adjustment procedure(s).

b) The pass/fail criteria, pertaining to each EA related to quantum optical components and the parameter adjustment procedure(s). The following considerations are related to the criteria:

    1) In some cases, effective IT-controls against some known attacks (related to the threats to quantum optical components) are well studied and recognized in the community, and vulnerabilities related to those attacks cannot be exploited if corresponding IT-controls have been adopted. The pass/fail criteria for these cases are explained as whether relevant IT-controls have been effectively implemented in the TOE. For example, the EA in 8.11 examines the ability of the TOE to resist double-click attacks, and the test passes if appropriate measures have been adopted and implemented.

2) In some cases, the security of the TOE is connected with some security-related technical parameters. That is, when the values of certain parameters exceed (or are less than) certain thresholds, it is possible the TOE includes some vulnerabilities that can be exploited by the adversary. In such cases, test procedures provide methods to measure concrete values for the parameters by examining the TOE. The pass/fail criteria in such EAs generally specify comparisons with given thresholds as the method to decide the evaluation result. For example, the EAs in 7.8, 7.9 and 8.4 examine the ability of the optical isolation component and the injected light monitor of the TOE, and make pass/fail verdicts based on the measured values of relevant parameters.

3) In some cases, the measured security-related technical parameters described in 2) can be incorporated into the privacy amplification process of the post-processing procedure to address the problem of potential information leakage caused by potential vulnerabilities. Where a developer claims to be doing so, after performing these EAs, the evaluator should also examine whether the thresholds used by the pass/fail criteria are correctly used in the privacy amplification process of the TOE. An example of these cases is the EA in 8.2.

EAs for these SFRs usually involve performing tests over some pre-defined parameter spaces specified by the input parameters of the EAs. Since most of the parameter spaces are continuous, this document adopts the strategy of evenly discretizing the parameter spaces and performing the test step by step. Alternatively, the tests may be performed by randomly probing the parameter space (such as in the EAs of 7.9, 8.5, 8.9, and 9.2).

With regard to performing tests for the EAs, evaluators shall take account of measurement errors. The normal objective is to ensure that sufficient data are measured to demonstrate that tests are passed in a statistically significant manner. However, in some EAs, the parameters shall be scanned in a range that may include regions where the probability of measuring events falls close to zero, such as near the edges of the active window of a gated detector. In such cases, it is not practical to measure sufficient data to ensure tests pass reliably over the entire range. Where appropriate, evaluators may state that such a test only fails if a pass/fail criterion is failed in a statistically significant manner after a reasonable amount of data has been recorded.

To clearly understand the relationship between EAs and known attacks against the QKD modules, see Table D.1.

5.3.4 EAs for SFRs on conventional network components

The evaluation of conventional network components is a relatively mature topic in the security evaluation community for conventional network devices. In order to remove unnecessary complexity and retain consistency with the methodologies in existing standards, this document does not define new evaluation activities for conventional network components unless necessary, and refers to existing standards or specifications wherever possible. The SFRs within the classes of FAU, FCS, FDP, FIA, and FMT, pertaining to the evaluation of security audit, cryptographic operation, RNG, and network-management functions respectively, can typically be evaluated by referring to existing methods, including those from ISO/IEC 18367, ISO/IEC 20543 and cPP for Network Devices.[6] See Clause 10 for further information.

5.3.5 Thresholds and input parameters related to the evaluation activities

For most of the EAs specified in this document, thresholds and input parameters have been defined in the test procedures and are used to specify the pass/fail criteria and the input constraints. The thresholds, input parameters, and relevant pass/fail criteria together constitute the basis for the evaluator issuing an evaluation verdict and shall be a necessary part of the evaluation method of QKD modules.

Since the primary objective of the document is to specify the general evaluation method for QKD modules, this document does not specify values for the thresholds and input parameters. Instead, the values of thresholds and input parameters are expected to be given in PPs, STs or anywhere recognized by the relevant evaluation authority. Specifically, they can be specified according to the expected