BS ISO/IEC 23837-2:2023

BSI Standards Publication

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

Part 2: Evaluation and testing methods

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 23837-2:2023

# National foreword

This British Standard is the UK implementation of ISO/IEC 23837-2:2023.

The UK participation in its preparation was entrusted to Technical Committee IST/33/3, Security Evaluation, Testing and Specification.

A list of organizations represented on this committee can be obtained on request to its committee manager.

**Contractual and legal considerations**

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

© The British Standards Institution 2023
Published by BSI Standards Limited 2023

ISBN 978 0 539 05956 4

ICS 35.030

**Compliance with a British Standard cannot confer immunity from legal obligations.**

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 October 2023.

**Amendments/corrigenda issued since publication**

| Date | Text affected |
|---|---|

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 23837-2:2023

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)

Documents
Document Sharing Hub
© ISO/IEC 2023

Full document details: BS ISO/IEC 23837-2:2023

**COPYRIGHT PROTECTED DOCUMENT**

© ISO/IEC 2023

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
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland



© ISO/IEC 2023 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 23837-2:2023

# Contents

Page

**Foreword** ... **vi**
**Introduction** ... **vii**
**1 Scope** ... **1**
**2 Normative references** ... **1**
**3 Terms and definitions** ... **1**
**4 Abbreviated terms** ... **3**
**5 Overview of the evaluation method for QKD modules** ... **4**
5.1 General ... 4
5.2 Scope of the evaluation method ... 4
5.3 Overview of evaluation activities for SFRs ... 5
5.3.1 General ... 5
5.3.2 EAs for SFRs FTP_QKD.1 and FTP_QKD.2 ... 6
5.3.3 EAs for SFRs on quantum optical components and parameter adjustment procedure(s) ... 6
5.3.4 EAs for SFRs on conventional network components ... 7
5.3.5 Thresholds and input parameters related to the evaluation activities ... 7
5.4 Overview of evaluation activities for SARs ... 8
**6 EAs for the evaluation of FTP_QKD** ... **8**
6.1 General ... 8
6.2 EA to test quantum state transmission and sifting procedures ... 10
6.2.1 General aspects ... 10
6.2.2 Test procedure ... 12
6.2.3 Pass/fail criteria ... 14
6.3 EA to test other post-processing procedures ... 14
6.3.1 General aspects ... 14
6.3.2 Test procedure ... 16
6.3.3 Pass/fail criteria ... 17
6.4 EA to test parameter adjustment procedure(s) ... 17
6.4.1 General aspects ... 17
6.4.2 Test procedure ... 19
6.4.3 Pass/fail criteria ... 19
**7 EAs for evaluating quantum optical components in the transmitter module** ... **19**
7.1 General ... 19
7.2 EA to test the photon-number distribution of optical pulses ... 22
7.2.1 General aspects ... 22
7.2.2 Test procedure ... 24
7.2.3 Pass/fail criteria ... 25
7.3 EA to test the mean photon number and stability of optical pulses ... 25
7.3.1 General aspects ... 25
7.3.2 Test procedure ... 26
7.3.3 Pass/fail criteria ... 28
7.4 EA to test the independence of the intensities of optical pulses ... 28
7.4.1 General aspects ... 28
7.4.2 Test procedure ... 29
7.4.3 Pass/fail criteria ... 30
7.5 EA to test the accuracy of state encoding ... 30
7.5.1 General aspects ... 30
7.5.2 Test procedure ... 31
7.5.3 Pass/fail criteria ... 32
7.6 EA to test the indistinguishability of encoded states ... 32
7.6.1 General aspects ... 32
7.6.2 Test procedure ... 34

AVA Documents
Document Sharing Hub

© ISO/IEC 2023 – All rights reserved


Full document details: BS ISO/IEC 23837-2:2023

7.6.3 Pass/fail criteria ... 35
7.7 EA to test the uniform distribution of the global phase of optical pulses ... 36
7.7.1 General aspects ... 36
7.7.2 Test procedure ... 37
7.7.3 Pass/fail criteria ... 38
7.8 EA to test the degree of optical isolation of the TX module ... 38
7.8.1 General aspects ... 38
7.8.2 Test procedure ... 40
7.8.3 Pass/fail criteria ... 40
7.9 EA to test the sensitivity of the injected light monitor in the TX module ... 40
7.9.1 General aspects ... 40
7.9.2 Test procedure ... 41
7.9.3 Pass/fail criteria ... 42
7.10 EA to test the robustness of the TX module against laser injection ... 42
7.10.1 General aspects ... 42
7.10.2 Test procedure ... 44
7.10.3 Pass/fail criteria ... 46

**8 EAs for the evaluation of quantum optical components in the receiver module ... 47**
8.1 General ... 47
8.2 EA to test the consistency of detection probability in the RX module ... 49
8.2.1 General aspects ... 49
8.2.2 Test procedure ... 51
8.2.3 Pass/fail criteria ... 51
8.3 EA to test information leakage of back-flashes from the RX module ... 52
8.3.1 General aspects ... 52
8.3.2 Test procedure ... 53
8.3.3 Pass/fail criteria ... 54
8.4 EA to test the degree of optical isolation of the RX module ... 54
8.4.1 General aspects ... 54
8.4.2 Test procedure ... 55
8.4.3 Pass/fail criteria ... 55
8.5 EA to test the sensitivity of the injected light monitor in the RX module ... 56
8.5.1 General aspects ... 56
8.5.2 Test procedure ... 57
8.5.3 Pass/fail criteria ... 57
8.6 EA to test the robustness of the RX module against bright light blinding ... 58
8.6.1 General aspects ... 58
8.6.2 Test procedure ... 59
8.6.3 Pass/fail criteria ... 60
8.7 EA to test the appropriateness of dead time settings of SPDs ... 60
8.7.1 General aspect ... 60
8.7.2 Test procedure ... 61
8.7.3 Pass/fail criteria ... 62
8.8 EA to test the temporal profile of the detection efficiency for SPDs ... 62
8.8.1 General aspects ... 62
8.8.2 Test procedure ... 63
8.8.3 Pass/fail criteria ... 63
8.9 EA to test the robustness of the RX module against laser injection ... 64
8.9.1 General aspects ... 64
8.9.2 Test procedure ... 65
8.9.3 Pass/fail criteria ... 66
8.10 EA to test the detection limits of homodyne detectors in the RX module ... 67
8.10.1 General aspects ... 67
8.10.2 Test procedure ... 67
8.10.3 Pass/fail criteria ... 68
8.11 EA to test the appropriateness of double-click event handling ... 68
8.11.1 General aspects ... 68
8.11.2 Test procedure ... 69

AVA Documents
Document Sharing Hub


© ISO/IEC 2023 – All rights reserved

Full document details: BS ISO/IEC 23837-2:2023

8.11.3 Pass/fail criteria ... 69

**9 EAs for the evaluation of parameter adjustment procedure(s) ... 69**
9.1 General ... 69
9.2 EA to test the inducibility of detection probability mismatch ... 70
9.2.1 General aspects ... 70
9.2.2 Test procedure ... 73
9.2.3 Pass/fail criteria ... 74
9.3 EA to test the correctness of shot noise alignment ... 74
9.3.1 General aspects ... 74
9.3.2 Test procedure ... 75
9.3.3 Pass/fail criteria ... 77

**10 Supplementary activities for the evaluation of SFRs on conventional network components ... 77**
10.1 General ... 77
10.2 Evaluation activities for FCS related SFRs overview ... 78
10.3 Evaluation activities for other SFRs overview ... 78

**11 Supplementary activities for SARs ... 78**
11.1 General ... 78
11.2 Supplementary activities for Class APE: Protection Profile evaluation ... 78
11.3 Supplementary activities for Class ASE: Security Target evaluation ... 80
11.4 Supplementary activities for Class ADV: Development ... 80
11.4.1 Supplementary activities for ADV_ARC ... 80
11.4.2 Supplementary activities for ADV_FSP ... 81
11.5 Supplementary activities for Class AGD: Guidance documents ... 82
11.5.1 Supplementary activities for AGD_OPE ... 82
11.5.2 Supplementary activities for AGD_PRE ... 83
11.6 Supplementary activities for Class ATE: Test ... 83
11.6.1 Supplementary activities for ATE_FUN ... 83
11.6.2 Supplementary activities for ATE_IND ... 84
11.7 Supplementary activities for Class AVA: Vulnerability assessment ... 85

**12 Conformance statement ... 88**
12.1 General ... 88
12.2 Conformance statement specific to evaluation activities for SFRs ... 88
12.3 Conformance statement specific to EAs for SARs ... 89

**Annex A** (informative) **Guidance on the calculation of attack potential for the evaluation of QKD modules ... 90**

**Annex B** (informative) **Rating examples for AVA attack potential computation ... 97**

**Annex C** (informative) **Thresholds collection ... 100**

**Annex D** (informative) **Correspondence between EAs and known attacks to quantum optical components and parameter adjustment procedure(s) of QKD modules ... 104**

**Bibliography ... 106**

© ISO/IEC 2023 – All rights reserved


Documents
Document Sharing Hub
Full document details: BS ISO/IEC 23837-2:2023

# 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.


© ISO/IEC 2023 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 23837-2:2023

# 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.

© ISO/IEC 2023 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 23837-2:2023

Documents
Document Sharing Hub

# 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

© ISO/IEC 2023 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 23837-2:2023

**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]


© ISO/IEC 2023 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 23837-2:2023

**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 |

© ISO/IEC 2023 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 23837-2:2023

# 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.

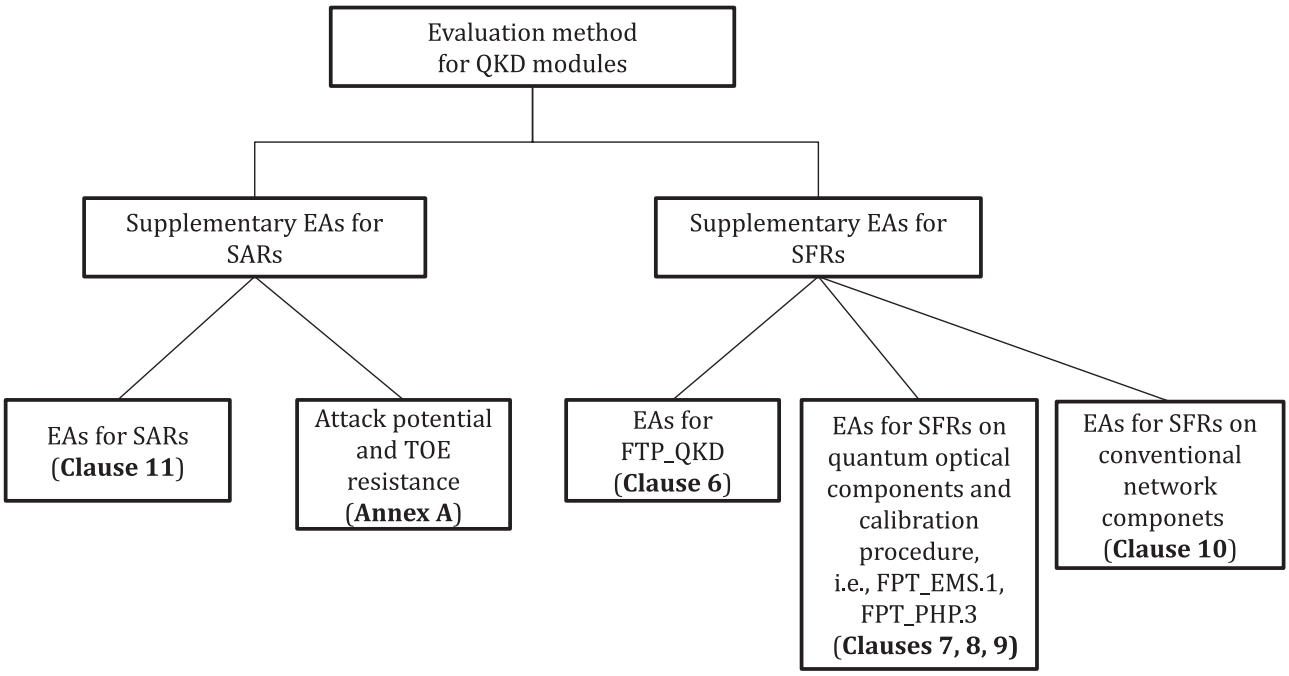



**Figure 1 — Structure of the specific EM for QKD modules and its constituent EAs**

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


© ISO/IEC 2023 – All rights reserved
Documents Document Sharing Hub
Full document details: BS ISO/IEC 23837-2:2023

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;

© ISO/IEC 2023 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 23837-2:2023

— 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.


© ISO/IEC 2023 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 23837-2:2023

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

© ISO/IEC 2023 – All rights reserved

AVA Documents Document Sharing Hub
Full document details: BS ISO/IEC 23837-2:2023

EAL of the evaluation. An evaluation authority can provide requirement(s) upon such values to the stakeholders (including the evaluators, developers, and users of QKD modules).

Tables C.1 and C.2 illustrate the thresholds distributed among the EAs.

As a convention of this document, the allowable ranges for some input parameters are described in the form of closed intervals, i.e. [*a*, *b*], where *a* and *b* are exact values depending on the context. For example, a tunable laser with a wavelength $\lambda$ in the range of $[\lambda_{min}, \lambda_{max}]$ means $\lambda_{min} \leq \lambda \leq \lambda_{max}$.

### 5.4 Overview of evaluation activities for SARs

The evaluator shall carry out a set of work units as specified in ISO/IEC 18045 to reach a verdict for the evaluation related to the assurance classes, families, and components (see ISO/IEC 15408-3). For security evaluation of QKD modules, supplementary evaluation activities are defined to make those generic work units described in ISO/IEC 18045 more specific by noting the characteristics of QKD modules, as described in Clause 11 in detail.

In principle, to meet the needs of the whole stack of pre-defined assurance levels from EAL 1 to EAL 7, all standardized assurance components specified in ISO/IEC 15408-3 should be scrutinized to supplement new evaluation activities for the evaluation of QKD modules. This document confines itself to only dealing with levels from EAL 1 to EAL 5+, where the augmentation of the security assurance component mainly focuses on AVA_VAN.5.

## 6 EAs for the evaluation of FTP_QKD

### 6.1 General

The SFRs on QKD protocol implementation are characterized by the extended functional family FTP_QKD, which captures the security requirements of the two essential stages of raw data generation (FTP_QKD.1) and post-processing (FTP_QKD.2). The EAs shown in Table 1 mainly focus upon the following aspects, with the general objective of examining the correctness of an implementation of the FUN_QKD functionality (or specifically the SFRs of FTP_QKD.1 and FTP_QKD.2):

— raw data generation;

— post-processing;

— parameter adjustment.


© ISO/IEC 2023 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 23837-2:2023

**Table 1 — EAs for the evaluation of FTP_QKD**

| Evaluation activity | Description | SFRs correspondence | Subclause index | Applicable protocols |
|---|---|---|---|---|
| Test quantum state transmission and sifting procedures | Test the correctness of functionality of the related generation of raw data between the TX module and the RX module, and the functionality of sifting of the resulting data when sifting is part of the QKD protocol. | FTP_QKD.1<br>FTP_QKD.2 | 6.2 | DV-PM-QKD;<br>DV-MDI-QKD;<br>DV-EB-QKD;<br>CV-PM-QKD;<br>CV-MDI-QKD;<br>CV-EB-QKD |
| Test other post-processing procedures | Test the correctness of the implementation of the post-processing procedures in the TOE, subsequent to any sifting that forms part of the QKD protocol. | FTP_QKD.2 | 6.3 | DV-PM-QKD;<br>DV-MDI-QKD;<br>DV-EB-QKD;<br>CV-PM-QKD;<br>CV-MDI-QKD;<br>CV-EB-QKD |
| Test parameter adjustment procedure(s) | Test the correctness of the implementation of the parameter adjustment procedure(s) in the TOE. | FTP_QKD.1 | 6.4 | DV-PM-QKD;<br>DV-MDI-QKD;<br>DV-EB-QKD;<br>CV-PM-QKD;<br>CV-MDI-QKD;<br>CV-EB-QKD |

The general requirements for carrying out these activities are as follows:

— required inputs in general, as described in 5.3.1;

— required tool types and setup in general: quantum channel related measurement equipment, network sniffer tools, post-processing emulator;

— required evaluator competences in general: the evaluator for this kind of EAs should be an expert in the optical measurements area;

— dependencies (in general): some of the EAs for FTP_QKD depend on the EAs for FPT_EMS.1/Quantum and FPT_PHP.3, which are detailed in Clauses 7, 8, and 9.

NOTE More specific requirements for each EA are added in 6.2 to 6.4 accordingly.

More information about the test and description of these EAs is given as follows:

a) Ideally, the security test procedures should be conducted on the QKD modules under test as a whole, without any adaptations. The objective of evaluation activities is to establish the security status of actual QKD modules under the conditions they can face in operation. In some instances, however, if the information gained from measuring the whole system is insufficient, it may be necessary to test individual components or sub-assemblies of QKD modules. Specifically, for the test of raw data generation and post-processing functions, the QKD modules under test shall be adapted to output a set of additional digital data to facilitate the access of some intermediates of protocol execution, which are needed to better perform the test, as detailed in the EAs in 6.2 and 6.3.

b) Since the EAs in Clause 6 are intended to test the correctness of the implementation of raw data generation and post-processing procedures, the tests are confined to being performed in an environment without adversarial intervention. More precisely, it is assumed that testing errors or faults that arise from noise were not maliciously introduced by an adversary.

© ISO/IEC 2023 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 23837-2:2023

c) For simplicity, the description of EAs in Clauses 6, 7, 8, and 9 mainly consider the implementation of DV-PM-QKD protocols. Although there are obvious differences between types of QKD protocols, the EAs in this document are designed and described in such a general way that:

1) those EAs described on the QKD transmitter modules can also be applied to the implementations of MDI-QKD protocols;

2) those EAs described on QKD receiver modules can also be applied to the implementations of EB-QKD protocols.

The applicability of each EA specified in this document is identified in general in the last column of Table 1 and in similar tables in Clauses 7, 8, and 9.

## 6.2 EA to test quantum state transmission and sifting procedures

### 6.2.1 General aspects

a) Objective of the evaluation activity

This EA intends to test the correctness of the functionality of raw data generation between the TX module and the RX module, and the functionality of sifting the resulting data when sifting is part of the QKD protocol. Although other post-processing procedures are evaluated under 6.3, sifting typically handles high data-rates that are comparable to the transmission frequency, so it is considered here.

NOTE The TOE does not include the quantum channel and classical channel connecting the QKD TX module and RX module, but only the relevant interfaces corresponding to the channels, as described in ISO/IEC 23837-1:2023, 6.4.2.

b) Required inputs

Besides the relevant documentation listed in the general input requirements, it is required to adapt the TOE (where not a capability of the TOE) to provide a set of additional digital data in order for the test to be performed. The data rates in the TX module can be high for some additional digital data. In many cases, the additional digital data that shall be output is generated at a rate that is a few times greater than the rate at which quantum states are emitted from the transmitter module, dependent upon the QKD protocol in operation. For this EA, it is sufficient for the TX and RX modules to retain additional digital data for finite durations and deliver these retrospectively to the evaluator. The retained duration may be shorter than the duration of a QKD session. Tests may be repeated where necessary to reduce statistical uncertainty in the results.

c) Required tool types and setup

If the module under test is a QKD transmitter, an RX emulator with known characteristics is required to be available and working well. Similarly, if the module under test is a QKD receiver, a TX emulator with known characteristics is required to be available and working well. An emulator is a tool with a known and trusted implementation of the raw data generation and sifting functionalities, which allows analysis of the TX (or the RX) module under test. In other words, the emulator does not undertake any security requirements, but the correctness of its implementation is expected to be suitable for the analysis of the TX (or the RX) module under test.

To conduct this EA, the evaluator shall have an emulator in advance. The emulator can be prepared by the evaluator or implemented and then provided by the QKD manufacturer or the industrial community for evaluation. Either way, the emulator should be recognized by the evaluation authority.

The schematic of the setup for testing the encoder functionality of the TX module under test is shown in Figure 2. In some implementations, the functionalities of the signal source and encoder may be implemented together rather than as separate components. The schematic of the setup for testing the decoder functionality of the RX module under test is shown in Figure 3. Figure 2 and Figure 3 show just one example of relevant internal components and connections, and implementations can differ. Digital output 3 (as shown in Figures 2 and 3) can be derived from the detector in implementations


© ISO/IEC 2023 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 23837-2:2023

using passive techniques for decoding quantum states. The emulator shall provide any signal required by the TX/RX module under test to perform the functions of raw data generation and sifting close to a normal mode of operation.

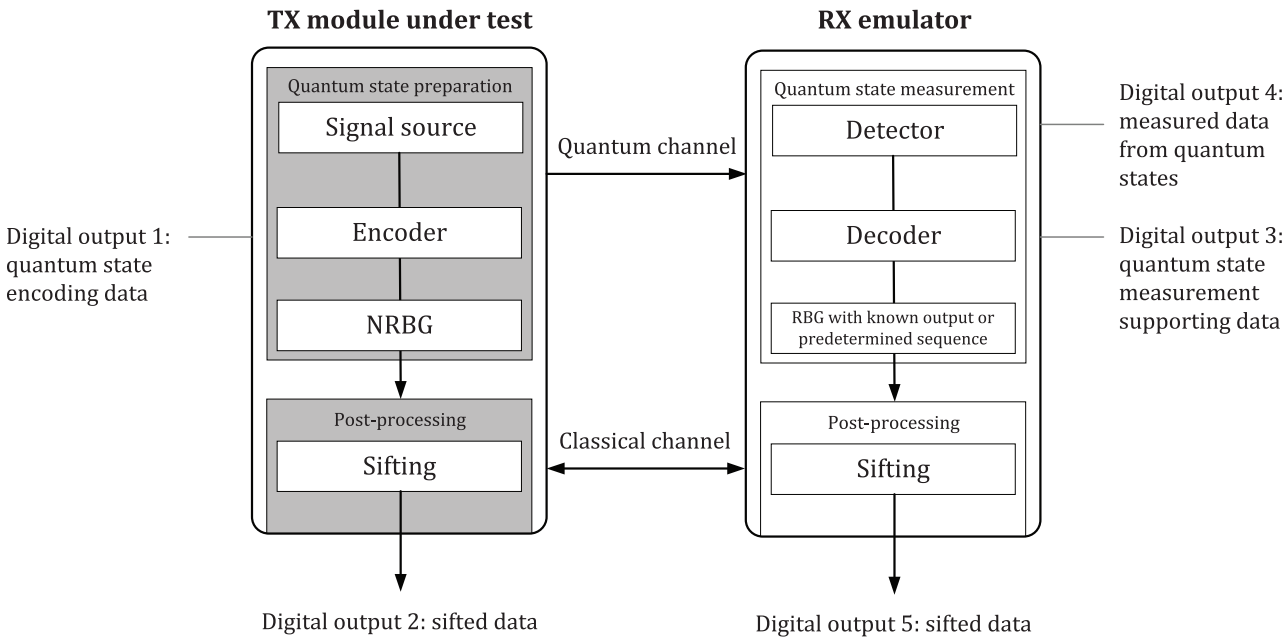



**Figure 2 — Setup for testing encoding and sifting functionalities of a TX module**

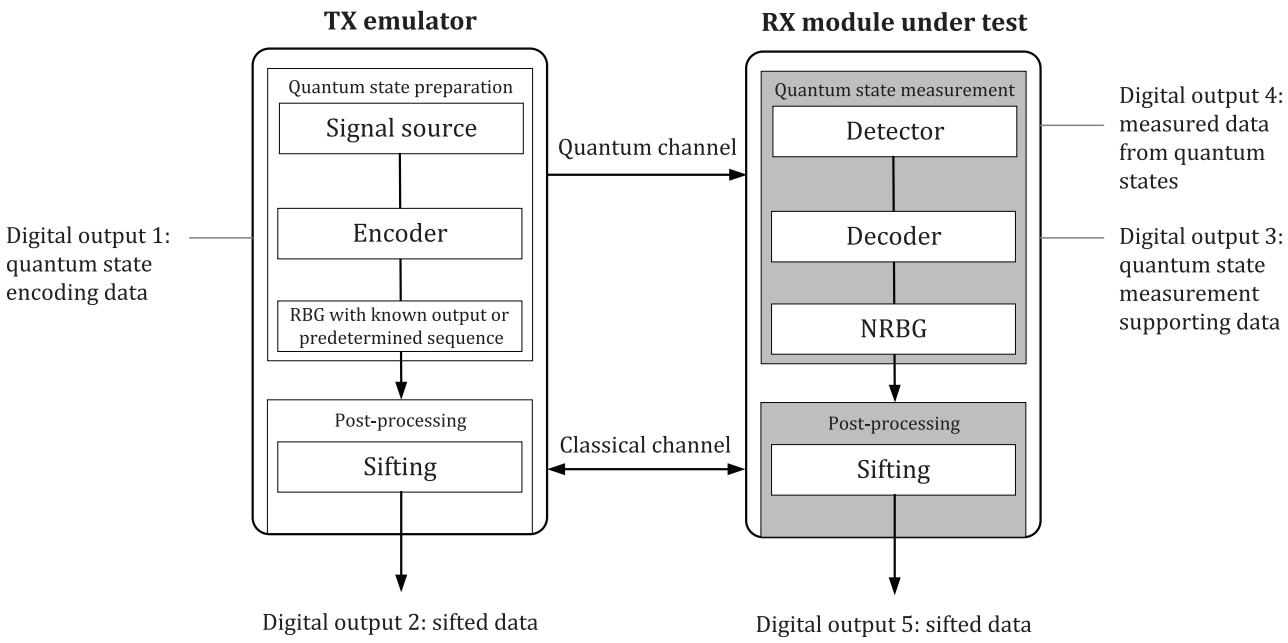



**Figure 3 — Setup for testing quantum state measurement and sifting functionalities of an RX module**

Figure 2 and Figure 3 do not show the whole structure of the QKD module under test and the emulator, but only the quantum state preparation/measurement and sifting components, since these are targets of the EA. This abstraction does not mean that other components are not necessary for the test. In fact, since the test is conducted on the QKD module under test as a whole, all components inside the QKD module under test are necessary and supposed to be in a normal running state apart from supplying the additional digital data required for the tests, so the results are representative of the real status of an actual QKD module.

© ISO/IEC 2023 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 23837-2:2023

While an NRBG is necessary for some protocols, it can be substituted by passive optical devices in others.

d) Rationale

The security of a QKD transmitter module crucially depends on the correct implementation of the protocol through the NRBG, signal source, and encoder. Similarly, the security of a QKD receiver module crucially depends on the correct implementation of the protocol through the NRBG, decoder, and detector. As a first step of the evaluation, it is necessary to examine the correct behaviour of these components in the system. The test procedure is based on knowledge of the random values used for encoding and measurement of quantum states (for relevant protocols). These can be used to determine whether the results of measurements of quantum states are statistically consistent with those expected if the QKD protocol had been implemented correctly within some threshold. By adapting the QKD module under test to allow access to the data used for preparing/measuring quantum states, the effectiveness of raw data generation and sifting functionalities in the module under test can be examined. Considering the typical lengths of the additional digital data that the QKD modules are configured to deliver, an input parameter $n_{\mathrm{exe}}$ denoting the execution times shall be assigned before conducting the EA. The input parameter is the number of sets of additional digital data that shall be evaluated for the tests in this EA to be statistically significant.

e) Dependencies

This EA has some dependencies on other EAs, including those on testing signal sources and detectors (see Clauses 7 and 8).

### 6.2.2 Test procedure

#### 6.2.2.1 QKD transmitter module

NOTE The digital outputs 1 to 5 are shown in Figures 2 and 3.

— Step 1: Prepare the environment for the test and connect the TX module under test and the RX emulator as required to perform the QKD protocol(s) to be evaluated. The initial step is to configure the TX module under test as the protocol requires. If the TX module under test is required to negotiate protocol configurations with its peer before executing the rest of the protocol, this shall be tested with the RX emulator before proceeding to the next step. Such configuration is often performed using purely conventional network components or specific to a protocol, and detailed activities are not discussed here.

— Step 2: Run the functionality under test. The TX module under test outputs from digital output 1 a set of quantum state encoding data that includes the necessary information used to encode quantum states over some test periods. For example, some simple discrete variable protocols that use two orthogonal states in each of two non-orthogonal bases output two bit-strings corresponding to the bit values and basis states used to encode quantum states. These are typically derived from the output of an NRBG. Intensity information is also required in some QKD protocols, such as protocols utilizing decoy states, or in some continuous variable protocols.

  In the RX emulator, any necessary information used to perform each measurement on a quantum state over some test period is made available through digital output 3. The measured data and any necessary timing information are made available through digital output 4. For example, the detector(s) register a photon for each quantum state for which detection occurred and the timings of those events.

— Step 3: Execute step 2 multiple times and accumulate the digital data from all digital outputs until the number of sets of data held is $n_{\mathrm{exe}}$. There may be gaps between the periods when each data set was collected, but each digital data set shall correspond to a consistent set of quantum states. Where there is more than one possible protocol configuration, repeat step 1 between data sets and ensure that all possible protocol configurations are covered during the test. Then end the test. If the number


© ISO/IEC 2023 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 23837-2:2023

of configurations is large, an appropriate sampling of configurations may be agreed with the evaluator.

— Step 4: The evaluator should review the quantum state encoding data output from digital output 1 and test whether the distribution of encoded states is consistent with the QKD protocol implemented by each of the protocol configurations tested in step 3. As a minimum, the evaluator shall test that each state occurs with the probably expected for the QKD protocol as configured after considering measurement and statistical errors.

— Step 5: Compare the sifted data from digital output 2 of the TX module under test against the full quantum state encoding data from its digital output 1 using knowledge from digital outputs 3 and 4 of the RX emulator. Test that any sifting required under the QKD protocol was implemented correctly by the TX module under test.

— Step 6: Compare the sifted data from the TX module under test received through digital output 2 with the sifted data from the RX emulator through digital output 5. The expected relationships between elements of the sifted data depends upon the QKD protocol and the evaluator shall test whether the sifted data relates as expected. For example, in many discrete variable protocols, the two sets of sifted data are strongly correlated bit strings, although in many cases, the sifted data from the TX module under test may include additional data, e.g. which quantum states were decoy or vacuum states. In this case, the overlap between the main string of sifted bit values encoded by the TX module under test and the measured sifted bit string from the RX emulator provides a check of whether the intended bit values were encoded. In such cases, the overlap can be calculated as the number of bits in the main sifted bit strings divided by the total length of the main sifted bit strings. More detailed tests of the quality of encoding of the individual quantum states themselves are described in Clause 7.

#### 6.2.2.2 QKD receiver module

— Step 1: Prepare the environment for the test and connect the TX emulator and the RX module under test as required to perform the QKD protocol(s) to be evaluated. The initial step is to configure the RX module as the protocol requires. If the RX module under test needs to negotiate protocol configurations with its peer before executing the rest of the protocol, this shall be tested with the TX emulator before proceeding to the next step. Often such configuration is performed using purely conventional network components or is specific to a protocol and detailed EAs are not discussed here.

— Step 2: Run the functionality under test. The TX emulator outputs from digital output 1 a set of quantum state encoding data that includes the necessary information used to encode quantum states over some test period.

  In the RX module under test, any necessary information used to perform each measurement on a quantum state over some test period should be made available through digital output 3. For example, where an NRBG is used to randomly configure the decoder to measure the quantum state in a protocol using two non-orthogonal bases, the random bit string used to configure the decoder should be output. The measured data itself, along with any necessary timing information, shall be available from digital output 4. For example, the detector(s) register a photon for each quantum state for which detection occurred and the timings of those events.

— Step 3: Execute step 2 multiple times and accumulate the digital data from all digital outputs until the number of sets of data held is $n_{\text{exe}}$. There may be gaps between the periods when each data set was collected, but each digital data set shall correspond to a consistent set of quantum states. Where there is more than one possible protocol configuration, repeat step 1 between data sets and ensure that all possible protocol configurations are covered during the test. If the number of configurations is large, an appropriate sampling of configurations may be agreed with the evaluator.

— Step 4: The evaluator should review the quantum state measurement supporting data output from digital output 3 and test whether the distribution of measurements performed is consistent with the QKD protocol implemented by each of the protocol configurations tested in step 3. As a

© ISO/IEC 2023 – All rights reserved

AVA Documents Document Sharing Hub
Full document details: BS ISO/IEC 23837-2:2023

minimum, the evaluator shall test that each configuration occurs with the probably expected for the QKD protocol as configured after considering measurement and statistical errors.

— Step 5: Compare the sifted data from digital output 5 of the RX module under test against the full measured data from quantum states from its digital output 4, using knowledge from its digital outputs 3 about the measurements performed and the quantum state encoding data from the TX emulator's digital output 1. Test that any sifting required under the QKD protocol was implemented correctly by the RX module under test.

— Step 6: Compare the sifted data from the RX module under test received through digital output 5 with the sifted data from the TX emulator through digital output 2. The expected relationships between elements of the sifted data depends upon the QKD protocol and the evaluator shall test whether the sifted data relates as expected. For example, in many discrete variable protocols, the two sets of sifted data include strongly correlated bit strings. In this case, the overlap between the main string of sifted bit values encoded by the TX emulator and the measured sifted bit string from the RX module under test provides a check of whether the measurements performed by the RX module under test were those intended. In such cases, overlap can be calculated as the number of bits in the main sifted bit strings divided by the total length of the main sifted bit strings. More detailed tests of the quality of the measurements performed on individual quantum states themselves are described in Clause 8.

### 6.2.3 Pass/fail criteria

The qualifying tests in steps 1, 4, and 5 shall be passed for both the TX module (see 6.2.2.1) and the RX module (see 6.2.2.2). Otherwise, the TOE fails the test.

In general, a set of thresholds shall be defined to appropriately compare the sifted data in step 6 for a particular protocol. For many protocols, the overlap between the TX and RX modules sifted bit strings and those of the corresponding RX and TX emulators, as defined in step 6 for each module type (see 6.2.2.1 and 6.2.2.2), is calculated over the accumulated data from $n_{\mathrm{exe}}$ sets of data. In this case, if both of the calculated overlaps are above a given threshold $T_{\mathrm{overlap}}$, then the TOE passes the test. Otherwise, it fails the test.

Table 2 lists the threshold pertaining to the pass/fail decision of the EA for such cases.

**Table 2 — Threshold for the pass/fail decision of the EA**

| No. | Threshold notation | Meaning of the threshold |
|---|---|---|
| 1 | $T_{\mathrm{overlap}}$ | The overlap between the main sifted data from the RX and TX modules corresponds to an agreement between the quantum states encoded and the results measured from the quantum states, when calculated for the accumulated data from $n_{\mathrm{exe}}$ sets of data. |

In some protocols, detailed reconciliation procedures are required before strong correlations are revealed in the sifted data. Where step 6 of the above test procedures would not provide suitable assurance of the correctness of the quantum state encoding and measurement, alternative tests referring to 6.3 may be considered.

## 6.3 EA to test other post-processing procedures

### 6.3.1 General aspects

a) Objective of the evaluation activity

This EA intends to examine the correctness of the implementation of other post-processing functions subsequent to any sifting that is part of the QKD protocol. Sifting is a post-processing procedure but is evaluated under 6.2.

b) Required inputs


© ISO/IEC 2023 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 23837-2:2023

Besides the relevant documentation listed in the general input requirement, it is required to adapt the TOE to output a set of additional digital data to perform the test. A set of additional digital data shall provide data corresponding to the entire QKD session duration to test post-processing procedures performed on the entire block of data from a QKD session. It is sufficient for the QKD modules to output the additional digital data retrospectively. Data before sifting is not required to be output for this EA. Tests may be repeated where necessary to reduce statistical uncertainty in the results.

In addition, a sufficiently long common QKD authentication key shall be shared initially between the QKD module under test and the emulator.

The QKD module under test may be adapted such that the pre-shared QKD authentication key is reused for each QKD session in the test. This can reduce the length of the pre-shared QKD authentication key required to one that is sufficient to run any single QKD session. It is also possible for each QKD session in the test to consume a new section of the pre-shared key. In this case, the key shall be long enough for the entire test in this case.

c) Required tool types and setup

If the module under test is a QKD transmitter, an RX emulator with known characteristics is required. Likewise, if the module under test is a QKD receiver, a TX emulator with known characteristics is required. An emulator is defined as a tool with a known and trusted implementation of the expected functionality, which allows analysis of the TX (or the RX) module under test.

To conduct this EA, the evaluator shall have an emulator in advance. The emulator can be prepared by the evaluator themselves or can be implemented and then provided by the QKD manufacturer or the industrial community for evaluation. Either way, the emulator should be generally recognized by the evaluation authority.

A schematic of a common setup for testing the post-processing functionality of the TX module under test is shown in Figure 4. Post-processing may be structured differently from this example and is not required to be performed in the order shown.

The test is conducted on complete QKD modules adapted to provide the necessary additional digital data. In this EA, the raw data input to the error correction component is derived from the output of any sifting procedure in post-processing procedures (as evaluated in 6.2). More explanation for the setup is given in the rationale [d)] of this EA. Accordingly, the setup for testing other post-processing functionality subsequent to any sifting procedure of the RX module is quite similar and not detailed in this schematic.

© ISO/IEC 2023 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 23837-2:2023

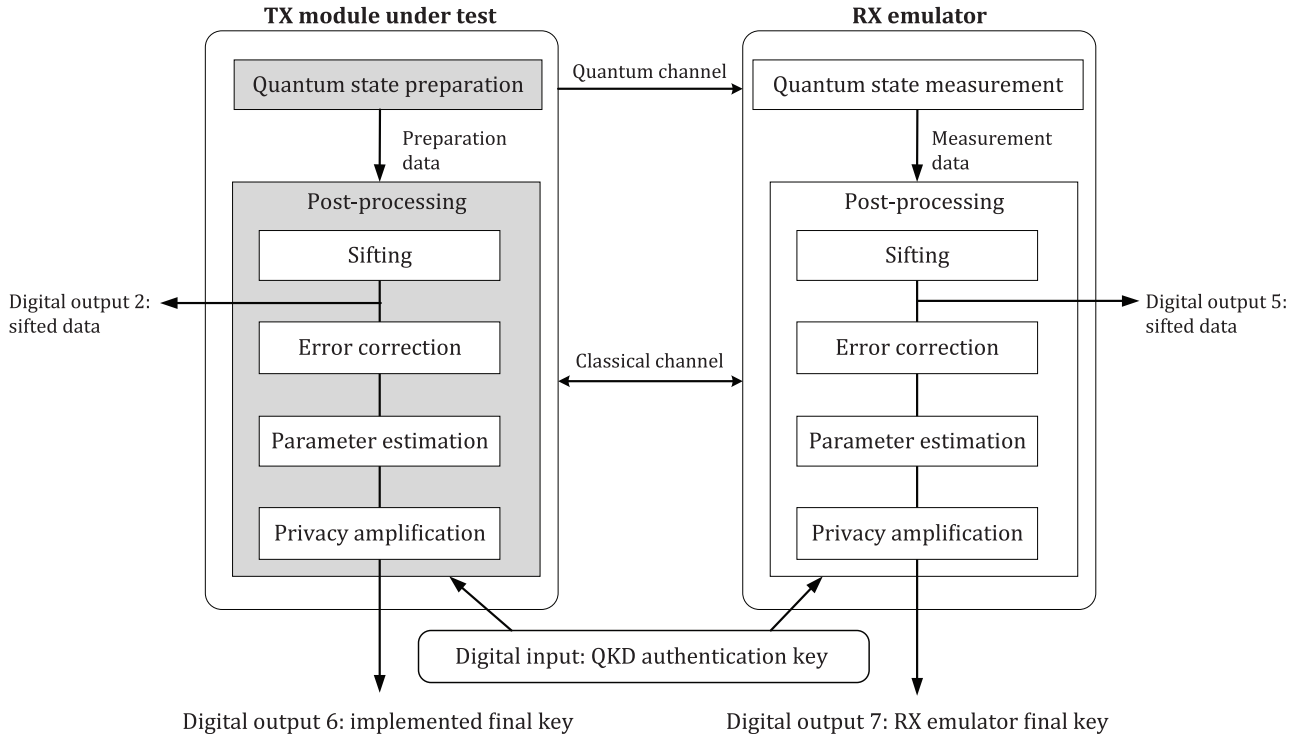



**Figure 4 — Schematic of the setup for testing the post-processing functionality of a TX module**

The sifting step is not required in some protocols, such as no switching CV QKD protocols. In this case, the output of quantum state preparation/measurement is used as the source for digital output 2 and digital output 5, respectively (see Figure 4).

In some cases, the post-processing procedures of a QKD protocol cannot be clearly separated and may be merged or run in parallel etc. Typically, parameter estimation begins earlier than shown and informs some parameters to error correction, but it also can use data from error correction.

d) Rationale

Since the QKD modules under test are operated as complete modules in the EA, the starting digital outputs for evaluating the subsequent post-processing components are derived from the output of the sifting procedure. An input parameter $n_{\mathrm{exe}}$ for this EA sets how many QKD sessions are required to be evaluated to ensure the test is statistically significant and shall be assigned before conducting the EA.

e) Dependencies

This EA shall be done after the quantum state transmission and sifting of post-processing procedures have been validated by passing the EA described in 6.2.

### 6.3.2 Test procedure

— Step 1: Prepare the environment for the test and connect the TX module under test and the RX emulator as required to perform the QKD protocol(s) to be evaluated. The initial step is to configure the TX module under test as the protocol requires.

— Step 2: Run a QKD session to generate final keys in the TX module under test and the RX emulator. The output of the TX module under test is recorded from digital output 6 and the input to the other post-processing procedures under test subsequent to the sifting procedure is recorded from digital output 2. The RX emulator final key is recorded as digital output 7 and the input to the post-processing procedures subsequent to the sifting procedure in the RX emulator is recorded from digital output 5.


© ISO/IEC 2023 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 23837-2:2023

NOTE The digital outputs 2, 5, 6, and 7 are shown in Figure 4.

— Step 3: Run step 1 to step 2 until $n_{exe}$ QKD sessions have been completed and the results recorded, and ensure all the possible protocol configurations have been covered during the test. Then run step 4 to step 8 below.

— Step 4: For each QKD session, perform the full post-processing procedure on the sifted data recorded from the TX module under test and the RX emulator independently from the TOE to generate a fully emulated final key. This can differ from the key from step 2 since entropy is introduced when the post-processing procedures is repeated independently.

— Step 5: For each QKD session, test whether the TX module under test in step 2 delivered a final key whenever the RX emulator delivered a final key, or whether both the TX module under test and the RX emulator aborted the session and delivered no final key.

— Step 6: For each QKD session, compare the length of the final key from the TX module under test with the length of the fully emulated final key from step 4 to check that parameter estimation resulted in an appropriate amount of privacy amplification. Test that the final keys from the TX module under test are not longer than the final keys from step 4 on average by a statistically significant amount.

— Step 7: Count the number of overlapping bits in all the final keys from step 2 where the implemented final key bit from the TX module matches the RX emulator final key bit. Calculate the overlapping fraction by dividing this by the total number of bits in all the final keys from the TX module.

— Step 8: Repeat steps 1 to 8 similarly but with the TX emulator connected to the RX module under test. Then end the test.

### 6.3.3 Pass/fail criteria

The qualifying tests in steps 5 and 6 and the repeat of these steps with the TX emulator and the RX module under test as in step 8 shall be passed. Otherwise, the TOE fails the test.

If the overlapping fraction calculated in step 7 and the repeat of this step with the TX emulator and the RX module under test as in step 8 are both above a given threshold $T_{PP}$ for post-processing, the test is passed. Otherwise, it fails. Table 3 lists the threshold pertaining to the pass/fail decision of the EA.

**Table 3 — Threshold for the pass/fail decision of the EA**

| No. | Threshold notation | Meaning of the threshold |
|---|---|---|
| 1 | $T_{PP}$ | The required minimum probability that the post-processing outputs or responses of the QKD module under test and the emulator are identical.<br>The threshold is common to the paired QKD transmitter and QKD receiver modules. |

NOTE The value of $T_{PP}$ can be set to be 1, which means that if the final keys are not identical the test fails.

## 6.4 EA to test parameter adjustment procedure(s)

### 6.4.1 General aspects

a) Objective of the evaluation activity

This EA intends to validate the correctness of the TOE in implementing the SFR elements on parameter adjustment (i.e. FTP_QKD.1.6, FTP_QKD.1.7, and FTP_QKD.1.8). Specifically, it intends to examine:

1) Can the TOE initiate the relevant parameter adjustment procedure(s) if trigger events occur during a QKD session?

© ISO/IEC 2023 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 23837-2:2023

2) Can the TOE preserve a secure state when parameter adjustment procedure(s) are triggered and refuse to run any QKD session(s) until the parameter adjustment procedure(s) terminates, unless the restrictions on execution allow it to run QKD sessions simultaneously?

3) Can the TOE indicate the status of any parameter adjustment procedure(s)?

NOTE This EA does not intend to examine whether the parameter adjustment procedure(s) can really realign system parameters or not. This is mainly because the set of system parameters related to parameter adjustment procedure(s) are various and depend on the specific implementation of QKD modules. Therefore, it is difficult for this document to specify a general testing method of it. Further, the function of parameter adjustment procedure(s) is usually the content of performance testing of QKD modules; the validity of parameter adjustments is therefore omitted from the scope of security evaluation specification of this document.

b) Required inputs

The developer shall provide an entire TOE, including the two QKD modules under test. In addition, the TOE shall be prepared (or adapted) to allow the evaluator to trigger the parameter adjustment procedure(s), request to run QKD sessions, and observe the status indication of parameter adjustment.

c) Required tool types and setup

The two QKD modules under test are connected normally (such that they can run QKD sessions as in the normal state), as shown in Figure 5 for the example of a PM-QKD protocol but the EA is not limited to such protocols.

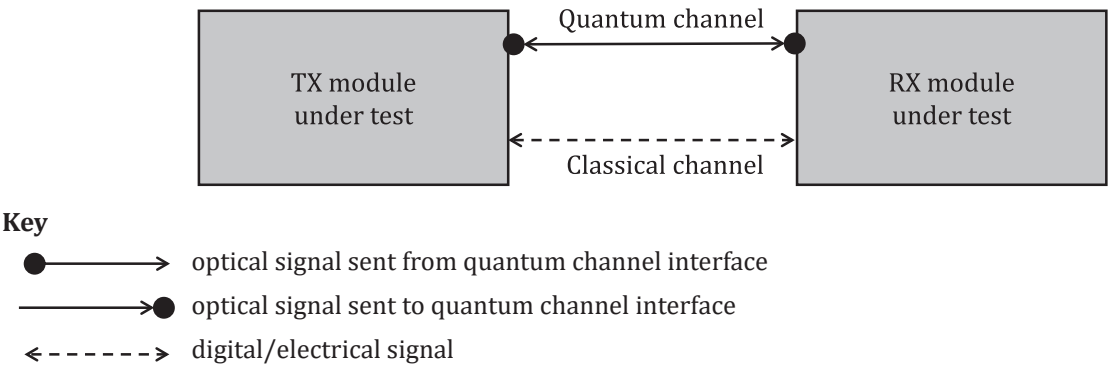



**Figure 5 — Schematic of the setup for testing the parameter adjustment procedure(s)**

d) Rationale

Generally, the parameter adjustment procedure(s) of QKD modules can be manually triggered by the administrator, or automatically triggered by accidental failure events during the execution of the TOE. The actual trigger conditions are defined by the PP/ST in SFR element FTP_QKD.1.6 as shown in ISO/IEC 23837-1:2023, 9.3.2. For general purposes, this EA does not describe the specific trigger methods, but just assumes the evaluator can apply them to trigger the parameter adjustment procedure(s) during the execution of the TOE, though for some implementation strategies of the TOE, it should be adapted to provide this support.

Then, by checking the indication or status information of the TOE, the evaluator can examine whether the parameter adjustment procedure(s) of the QKD system is triggered or not. The indication method is specified by the PP or ST of the TOE in FTP_QKD.1.8, as shown in ISO/IEC 23837-1:2023, 9.3.2.

To examine whether the TOE refuses to run any QKD session before the end of any parameter adjustment procedure(s) that is not allowed to run simultaneously with QKD session(s), the evaluator asks the TOE to run QKD sessions during the procedure and checks the reaction of the TOE. For general purposes, this EA does not describe the methods of requesting the TOE to run QKD sessions, but assumes the


© ISO/IEC 2023 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 23837-2:2023

QKD modules under test can support the intention of the evaluator (which generally can be achieved by adapting the TOE somehow).

e) Dependencies

The EAs related to parameter adjustment procedure(s) are specified in two places in this document. In detail, the EA for examining the correct implementation of parameter adjustment procedure(s) is presented in 6.4, while the EA for examining the effectiveness of the IT-related controls to resist known attacks against parameter adjustment procedure(s) are presented in 9.2. The EA specified in 6.4 should be conducted before the EA in 9.2, and the EAs specified in 6.2 and 6.3 should be conducted before the EA in 6.4.

### 6.4.2 Test procedure

— Step 1: Run the TOE to perform QKD sessions.

— Step 2: For each trigger method assigned in the SFR element of FTP_QKD.1.6, apply it to trigger the parameter adjustment procedure(s), and do the following test until all cases have been tested:

  a) Observe the status changes of the TOE in order to validate whether the TOE can initiate the parameter adjustment procedure(s), and whether the TOE stops the on-going QKD session where the parameter adjustment procedure is not allowed to run simultaneously with QKD session(s) and indicates to the operator about the situation appropriately.

  b) During the parameter adjustment procedure(s), request that the TOE run a QKD session and examine whether the TOE refuses to execute it.

  c) When the parameter adjustment procedure(s) is finished, examine whether the TOE can run QKD sessions normally.

### 6.4.3 Pass/fail criteria

The test is passed if, for each trigger method assigned in the SFR element of FTP_QKD.1.6, the following conditions are satisfied together. Otherwise, the test has failed.

a) Each trigger method is effective in triggering the parameter adjustment procedure(s).

b) Before commencing a parameter adjustment procedure that is not allowed to run simultaneously with QKD session(s), the on-going QKD session is terminated and the relevant keying material generated during the relevant sessions is handled appropriately.

c) The TOE indicates the status of parameter adjustment procedure(s) in an appropriate way as defined in the SFR element FTP_QKD.1.8 and refuses to execute QKD sessions during the parameter adjustment procedure(s) that are not allowed to run simultaneously with QKD session(s).

d) When the parameter adjustment procedure(s) terminates successfully, QKD sessions can be executed as in the normal state.

There is no threshold pertaining to the pass/fail decision defined in the EA.

# 7 EAs for evaluating quantum optical components in the transmitter module

## 7.1 General

The EAs for the security evaluation of quantum optical components in TX modules are listed in Table 4. These EAs address potential flaws in quantum optical components of QKD modules that, if present, can otherwise compromise the security functions realizing the two security requirements FPT_EMS.1/Quantum and FPT_PHP.3. These flaws are known security-related issues of (or attacks against) TX modules that have been published and peer reviewed in academic literature. Although not all types of attacks have been demonstrated to date, at least a strategy for each type of attack has been identified.

© ISO/IEC 2023 – All rights reserved

AVA Documents Document Sharing Hub
Full document details: BS ISO/IEC 23837-2:2023

**Table 4 — EAs for quantum optical components in a TX module**

| Evaluation activity | Description | SFRs correspondence | Subclause index | Applicable protocols |
|---|---|---|---|---|
| Test the photon-number distribution of optical pulses | Test if emissions are consistent with the photon number distribution(s) of the optical pulses that are expected to be emitted by the TX module under test. | FPT_EMS.1/Quantum | 7.2 | DV-PM-QKD; DV-MDI-QKD; CV-PM-QKD; CV-MDI-QKD |
| Test the mean photon number and stability of optical pulses | Test if the mean photon number of the optical pulses generated in the TX module under test, as well as its stability in time are consistent with the requirements of the implemented QKD protocol. | FPT_EMS.1/Quantum | 7.3 | DV-PM-QKD; DV-MDI-QKD; CV-PM-QKD; CV-MDI-QKD |
| Test the independence of the intensities of optical pulses | Test if the intensities of the emitted pulses for each intended intensity are independent of the underlying intensity modulation pattern. | FPT_EMS.1/Quantum | 7.4 | DV-PM-QKD; DV-MDI-QKD; CV-PM-QKD; CV-MDI-QKD |
| Test the accuracy of state encoding | Test if the quantum states emitted by the TX module under test are encoded sufficiently accurately to match those required by the implemented QKD protocol. | FPT_EMS.1/Quantum | 7.5 | DV-PM-QKD; DV-MDI-QKD |
| Test the indistinguishability of encoded states | Test if the different quantum states encoded in a same degree of freedom can be distinguished from the perspective of non-encoding degrees of freedom. | FPT_EMS.1/Quantum | 7.6 | DV-PM-QKD; DV-MDI-QKD; CV-PM-QKD; CV-MDI-QKD |
| Test the uniform distribution of the global phase of optical pulses | Test if the global phase of optical pulses is randomly distributed, as required by the implemented QKD protocol. | FPT_EMS.1/Quantum | 7.7 | DV-PM-QKD; DV-MDI-QKD; |
| Test the degree of optical isolation of the TX module | Test if the isolation ability provided by the TX module under test suffices to prevent the light injected from the quantum channel to the module. | FPT_PHP.3 | 7.8 | DV-PM-QKD; DV-MDI-QKD; CV-PM-QKD; CV-MDI-QKD |
| Test the sensitivity of the injected light monitor in the TX module | Test if the injected light monitor deployed to detect light injected by an adversary through the quantum channel interface works properly. Characterize its sensitivity under continuous-wave emission and high-frequency/narrow-width optical pulses. | FPT_PHP.3 | 7.9 | DV-PM-QKD; DV-MDI-QKD; CV-PM-QKD; CV-MDI-QKD |
| Test the robustness of the TX module against laser injection | Test the robustness of the TX module under test against laser light injected through the quantum channel interface. | FPT_PHP.3 | 7.10 | DV-PM-QKD; DV-MDI-QKD; CV-PM-QKD; CV-MDI-QKD |

a) General description of inputs

The TX module should be operated under conditions that are as close to normal operating conditions as possible, which means the security test procedures should be conducted on the TX module as a whole, without requiring additional interfaces, channels, or outputs other than those already present in the


© ISO/IEC 2023 – All rights reserved
AVA Documents Document Sharing Hub
Full document details: BS ISO/IEC 23837-2:2023

TX module. Its objective is to reflect the security status of actual QKD modules under the conditions they face in operation.

Some of the EAs mentioned in Clause 7 require the TX module under test to be configured to emit pulses equivalent to those in the raw data generation stage. Here "equivalent" means:

— Pulses are transmitted with intensities used in the raw data generation stage.

— Pulses are encoded with a random sequence used in the raw data generation stage.

— For QKD protocols in which the TX module under test is required to emit optical pulses of more than one intensity, pulses are modulated to a sequence of intensity states used in the raw data generation stage.

In order to conduct the EM effectively, EAs may allow more modifications to the TOE, for example:

— In a limited number of instances, if the information gained from measuring the whole system is insufficient, individual components or sub-assemblies of QKD modules may be tested (see 7.8).

— Where a TX module supports reducing its internal attenuation in a test mode, the attenuation inside the TX module may be reduced such that the optical pulses can be emitted at a higher average intensity level than in the raw data generation stage, in order to relax the sensitivity requirements of test tools and/or to reduce the duration of measurements (see 7.4, 7.6, 7.7, and 7.10).

— Digital output indicating the order of states emitted from the TX module may be enabled where needed to analyse the measurement result of those states (see 7.2 to 7.7 and 7.10).

— The TX module may be configured to emit an appropriate repeating pattern of states that is known to the evaluator. Such repeating patterns should typically be representative of patterns used in operation so that results are representative of the TX module in operation.

— A specially configured TX module may be used, e.g. to ignore repeated failures without transitioning to a failure state for the duration of an EA.

Where an EA requires modifying the operation of a TX module, the modification should be specified in the description of required inputs of the EA. It is implicitly assumed that the modification is removed or disabled after testing.

b) General description of test tools and setup

When performing the EAs in 7.2 to 7.10, the evaluator shall set up the test following best engineering practice and considering the specific characteristics of the instruments used. For example, SPDs are selected with a suitable clock rate, dead time, and noise level to perform the measurement on the TX module under test. The QKD protocol and design of the QKD modules can influence the detectors that are suitable for testing a given TX module. When planning the tests and analysing the results, the details of the performance of the detectors used should be considered, including dark counts, after pulses and time jitter that can occur during measurements. Any corrections made to account for the non-ideal behaviour of instruments shall be reasonable. Care shall be taken to ensure that corrections are performed in a manner that does not compromise the objectives of the EAs.

For those EAs that require the TX module to emit pulses equivalent to those in the raw data generation stage, the TX module can often do this only when connected to a compatible RX module. In such cases, it is appropriate to introduce an RX emulator to provide the signals expected by the TX module under test to enable it to be operated as required. Specifically:

— The RX emulator can supply trigger signals to the TX module under test and other test tools, or receive trigger signals from other tools.

— The required timing signals can be derived from signals present in the optical link between the TX module under test and the RX emulator.

© ISO/IEC 2023 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 23837-2:2023

— The optimal way to combine or split communications between a TX module under test and an RX emulator and signals to/from other tools depends upon the EA and details of the TX module under test. Optical couplers or wavelength multiplexing devices are usually suitable.

In some cases, an RX module under test can be used as an RX emulator.

## 7.2 EA to test the photon-number distribution of optical pulses

### 7.2.1 General aspects

a) Objective of the evaluation activity

This EA intends to test whether emissions are consistent with the photon number distribution(s) of the optical pulses that are expected to be emitted by the TX module under test.

b) Required inputs

The developer shall provide the TX module under test, which is configured to emit pulses equivalent to those emitted in the raw data generation stage. The TX module under test shall allow the evaluator to access time tagged digital data containing the intensity modulation pattern used by the TX module during the test.

c) Required tool types and setup

The evaluator shall prepare a 1 × $S$ beam splitter (BS) or equivalently a cascade of BS to realize the same 1 × $S$ splitting function. The input of the BS is connected to the quantum channel, which is connected on the other end to the quantum channel interface of the TX module under test. The output ports of the BS are connected to $S$ single-photon detectors ($SPD_1$, ..., $SPD_S$), whose outputs are connected to timing electronics capable of counting coincidences.

In this EA, a $k$-coincidence is taken to be the occurrence of a detection event in $k$ of the SPDs at times that are consistent with the arrival of a particular quantum state from the TX module at each SPD after considering jitter and latency. For gated SPDs, this may be taken as the occurrence of a detection event in $k$ of the SPDs in detector gates that are consistent with the arrival of a particular quantum state from the TX module at each SPD.

The output of the timing electronics is used to calculate the $k$-th order correlation function $g^{(k)}(t)$ at zero delay ($t$ = 0), where $k \in \{2,3,...,S\}$ is an integer representing the order of the correlation function, which is upper bounded by $S$ and decided by the evaluator, and $t$ is a time delay. The evaluator shall also prepare timing electronics to time tag the output of SPDs and a tool for the digital time analysis of the digital data coming from the TX module under test and the timing electronics.

The schematic of the setup for performing the EA is a generalized Hanbury-Brown-Twiss interferometer, as shown in Figure 6.


© ISO/IEC 2023 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 23837-2:2023

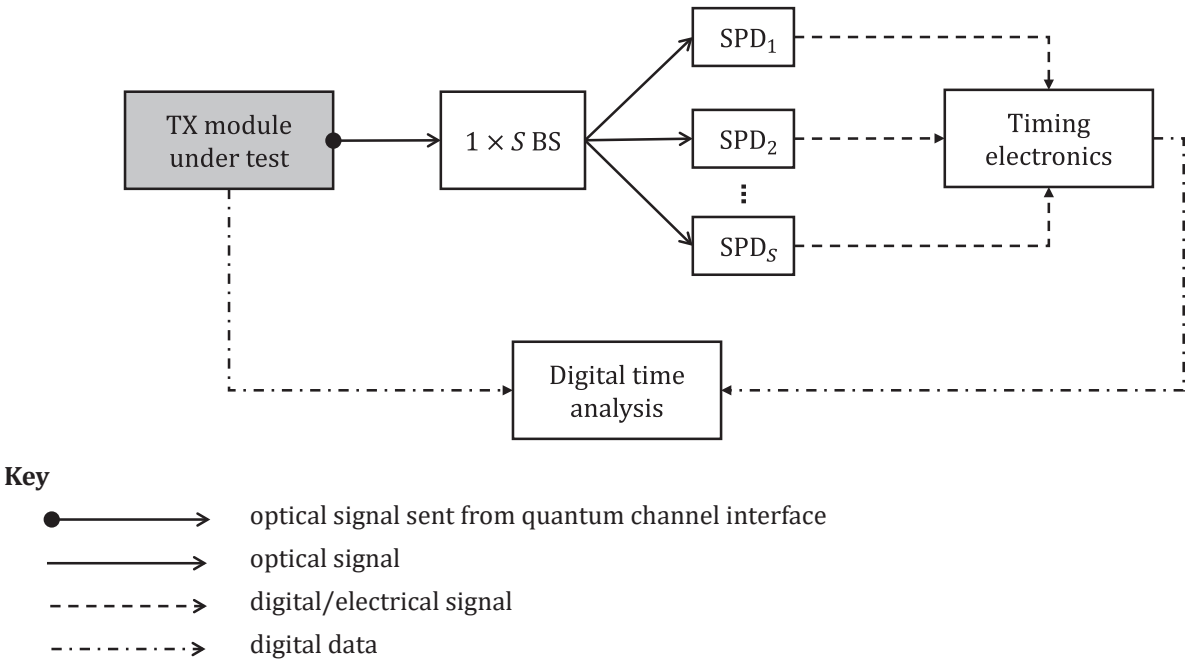



**Figure 6 — Schematic of the setup for testing the photon-number distribution of optical pulses**

d) Rationale

The photon number distribution(s), $P(m)$, of the optical pulses represents the probabilities that a pulse contains $m$ photons. The outcome of the test shall indicate whether the $P(m)$ measured from the TX module under test follows the theoretical distribution assumed in the QKD protocol. However, rather than testing $P(m)$ directly, the evaluator shall test correlation functions $g^{(k)}(t=0)$, with $k$ an integer larger than 1. There is a known relation between the photon number distribution, $P(m)$, and the correlation functions $g^{(k)}(0)$ at zero delay, which is denoted by $g^{(k)}$ for simplicity in this EA.

For the case of $k$ = 2, for example, the correlation function can be expressed as Formula (1)

$$g^{(2)} = \sum_m P(m)[m(m-1)]/\mu^2 \tag{1}$$

where

| | |
|---|---|
| $\mu$ | is the mean number of photons in an optical pulse, which is measured in another evaluation activity (see 7.3); |
| $m$ | is the photon number of an optical pulse; |
| $g^{(2)}$ | is the second order correlation function at zero delay. |

Thus, the correlation functions $g^{(k)}$ indirectly indicate whether the emitted photon number distribution follows the theoretical distribution expected under the QKD protocol. The SPDs produce "clicks" recorded by the timing electronics together with their time tags. Simultaneous clicks from $SPD_1$ and $SPD_2$ are used in determining $g^{(2)}$. Simultaneous clicks from $SPD_1$, $SPD_2$, and $SPD_3$ are used in determining $g^{(3)}$. In general, the simultaneous clicks from SPDs from 1 to $k$ are used in determining $g^{(k)}$. If the deviations between the measured $g^{(k)}$ and the theoretical values are within certain thresholds, it means the photon number distribution follows the theoretical distribution within a certain tolerance and this EA's test has passed.

© ISO/IEC 2023 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 23837-2:2023

If the TX module under test is required to emit more than one intensity of optical pulse under the QKD protocol, the evaluator can use the time tags registered by the timing electronics to correlate the clicks of the detectors with the intensities emitted by the TX module under test. This allows the evaluator to infer the $g^{(k)}$ functions for each of the intensities set by the TX module under test while operating a particular QKD protocol.

Clause 12 permits this EA to be replaced with an alternative EA using a different measurement method to estimate the photon number distribution $P(m)$. For example, measurements using a photon-number-resolving detector would be a possible basis for an alternative EA.

### 7.2.2 Test procedure

The test procedure below is described for the case where the QKD protocol requires the TX module to emit optical pulses with a single intensity. If more than one intensity is emitted, the evaluator shall repeat the analysis in steps 4 to 7 of the test procedure described below for each intensity, considering only the relevant optical pulses in each analysis.

— Step 1: Turn on the TX module under test and configure it to emit pulses equivalent to those in the raw data generation stage.

— Step 2: Where gated SPDs are used, adjust the timing of signals used to trigger the SPDs such that the optical pulses from the TX module under test arrive during the gates of the SPDs.

— Step 3: Record the number of optical pulses, $N_{\text{pulse}}$, emitted for an acquisition time that is long enough to obtain sufficient $S$-coincidence counts in the SPDs from 1 to $S$ to determine the $S$–1 deviations in Step 7 to the required precision.

— Step 4: Record the number of single clicks from SPDs in Figure 6 and denote by $N_1$, $N_2$, ..., $N_S$, and record the number of $k$-coincidence counts from the first $k$ SPDs in Figure 6 and denote by $N_{\text{c}}^{(k)}$ with $k \in \{2,3,...,S\}$.

NOTE 1 In most cases, measuring $g^{(k)}$ up to $k$ = 4 is sufficient to determine the photon number distribution of the TX module tightly.

NOTE 2 The $k$-coincidence counts also can be estimated from an appropriate combination of detection outcomes of the SPDs. For example, for $S$ = 4, it is possible to estimate $N_{\text{c}}^{(2)}$ from the detection outcomes of detector groups {12, 13, 14, 23, 24, 34}, $N_{\text{c}}^{(3)}$ from detector groups {123, 124, 134, 234} and $N_{\text{c}}^{(4)}$ from detector group {1234}.

— Step 5: Calculate the single count probability from the $i$-th SPD as $P_i = N_i / N_{\text{pulse}}$ and the coincidence count probability from the first $k$ SPDs as $P_{\text{c}}^{(k)} = N_{\text{c}}^{(k)} / N_{\text{pulse}}$ with $k \in \{2,3,...,S\}$.

— Step 6: Calculate the measured value of the correlation functions up to the order $S$, as Formula (2):

$$g_{\text{M}}^{(k)} = \frac{P_{\text{c}}^{(k)}}{P_1 P_2 \cdots P_k} \tag{2}$$

where $k \in \{2,3,...,S\}$.

— Step 7: Calculate the deviations between the measured $g_{\text{M}}^{(k)}$ obtained in the previous step and the theoretical $g_{\text{T}}^{(k)}$ expected for the TX module under test, as Formula (3):

$$\Delta^{(k)} = \left| g_{\text{M}}^{(k)} - g_{\text{T}}^{(k)} \right| \tag{3}$$


© ISO/IEC 2023 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 23837-2:2023

where $k \in \{2,3,...,S\}$.

### 7.2.3 Pass/fail criteria

If the TX module under test is operating a QKD protocol that only requires the emission of optical pulses into the quantum channel of equal intensity, then if each measured $\Delta^{(k)}$ is smaller than the $k$-th threshold value $T_{\mathrm{diffCor}(k)}$, the test has passed. Otherwise, the test has failed.

If a QKD protocol requires the TX module to emit more than one intensity of optical pulse into the quantum channel, the developer may optionally indicate a different $T_{\mathrm{diffCor}(k)}$ for each intensity or may indicate that the same threshold applies to all intensities. Some QKD protocols require such TX modules to emit with a certain probability pulses of very small intensity, corresponding to an approximation to the "vacuum" state. For these special states, moderate deviations in the photon number statistics are typically not very significant in the overall security analysis and obtaining a statistically significant measure of $\Delta^{(k)}$ may not be practical. If each measured $\Delta^{(k)}$ calculated for each subset of optical pulses, corresponding to a different intensity in the QKD protocol other than any "vacuum" state, is smaller than the relevant $k$-th threshold value $T_{\mathrm{diffCor}(k)}$ for that intensity, the test has passed. Otherwise, the test has failed.

Table 5 lists the threshold pertaining to the pass/fail decision of the EA.

**Table 5 — Threshold for the pass/fail decision of the EA**

| No. | Threshold notation | Meaning of the threshold |
|---|---|---|
| 1 | $T_{\mathrm{diffCor}(k)}$ | The absolute value of the difference between the measured value and the theoretical value of the $k$-th order correlation function, for a fixed intensity of the pulses emitted by the TX module. Where a QKD protocol requires the TX module to emit pulses of more than one intensity different thresholds may optionally be indicated for different intensities. |

## 7.3 EA to test the mean photon number and stability of optical pulses

### 7.3.1 General aspects

a) Objective of the evaluation activity

This EA intends to test the mean photon number of the optical pulses generated in the TX module under test, as well as its stability in time. The testing outcome indicates whether the mean photon number of the optical pulses falls consistently within the expected threshold limits.

b) Required inputs

The developer shall provide a TX module under test, which is configured to emit pulses equivalent to those emitted in the raw data generation stage. The TX module under test shall allow the evaluator to access time tagged digital data containing the intensity modulation pattern used by the TX module during the test.

c) Required tool types and setup

The evaluator shall prepare a calibrated optical detector that works below its saturation level and above its intrinsic noise level with known detection efficiency, $\eta_{\mathrm{det}}$, which shall be connected to the quantum channel interface of the TX module under test via a calibrated link of known transmissivity, $\eta$. The detector shall be sensitive to the output of the TX module under test.

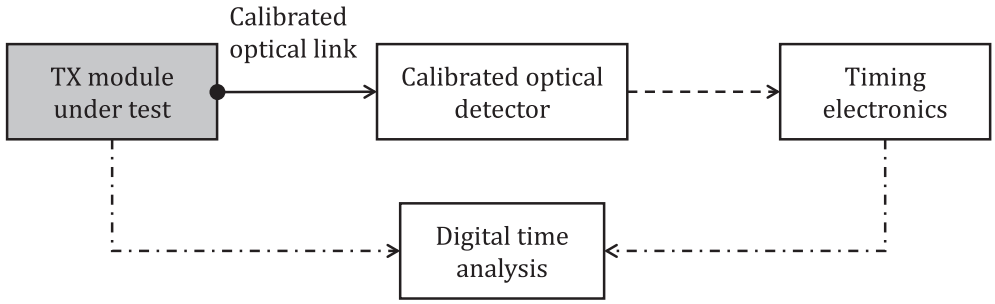
© ISO/IEC 2023 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 23837-2:2023

The evaluator shall also prepare timing electronics to time tag the output of the calibrated optical detector and a tool for the digital time analysis of the digital data coming from the TX module under test and the timing electronics.

NOTE A detector typically works best if it is well within its dynamic range, i.e. well below its saturation level and well above its intrinsic noise level. It is noted that for single photon detectors, the assumption that the intensity is proportional to the number of detection events counted is only reasonable under such conditions.

The schematic of the setup for performing the EA is shown in Figure 7.




**Key**

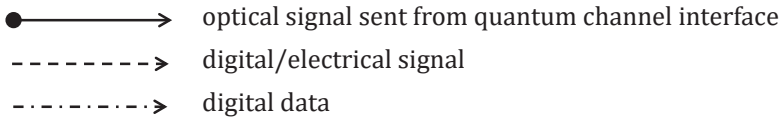



**Figure 7 — Schematic of the setup for testing the mean photon number and stability of optical pulses**

d) Rationale

This EA checks the mean photon number of the optical pulses generated and emitted by the TX module under test. It performs the measurement repeatedly over a period of time to assess the stability of the mean photon number. The TX module under test emits optical pulses with $K$ intensity levels, where $K$ is an integer number. The mean photon number is equivalent to knowing the intensity, where other information about the optical pulses, such as their wavelength and speed, is also known.

The calibrated optical detector may measure either the pulse energy or, for a single photon detector, whether or not a detection event was registered for each optical pulse. For an intensity $k$, the average pulse energy, $E_k$, is derived from summing the total energy, $I_k$, in each relevant pulse and dividing by the number of relevant pulses, $N_k$. Alternatively, the mean photon number, $\mu_k$, is derived from counting the total number of relevant photon detection events, $C_k$, and dividing the number of relevant pulses, $N_k$.

The measurement is repeated $M$ times and the average pulse energy or mean photon number for each measurement is checked against the threshold limit after correction for transmission loss and detector efficiency.

### 7.3.2 Test procedure

— Step 1: Turn on the TX module under test and configure it to emit pulses equivalent to those emitted in the raw data generation stage and connect it to the calibrated optical detector with detection efficiency, $\eta_{\text{det}}$, through a calibrated link of known transmission efficiency, $\eta$. If necessary, calibrated attenuation may be introduced before the calibrated optical detector to reduce the intensity to $f$ times the intensity emitted by the TX module, such that the intensities incident on the detector are in the calibrated range over which the detector is designed to operate. If a gated calibrated detector is used, adjust the timing of the gates such that the optical pulses arrive during the gates of the detector and synchronize the output with the timing electronics if necessary.


© ISO/IEC 2023 – All rights reserved
AVA Documents Document Sharing Hub
Full document details: BS ISO/IEC 23837-2:2023