INTERNATIONAL STANDARD

ISO/IEC 23837-2

First edition
2023-09

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

Part 2: Evaluation and testing methods

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

Partie 2: Méthodes d'essais et d'évaluation

Reference number
ISO/IEC 23837-2:2023(E)

© ISO/IEC 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

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

© ISO/IEC 2023 – All rights reserved

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

© ISO/IEC 2023 – All rights reserved

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

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

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

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