

ISO/IEC DIS 23837-2:20222023(E)

ISO/IEC JTC 1/SC 27/WG 3

Date: 2023-01-1206-20

Information security — Security requirements, test and evaluation methods for quantum key distribution — Part 2: ~~TestEvaluation~~ and ~~evaluationtesting~~ methods

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC 23837-2

<https://standards.iteh.ai/catalog/standards/sist/654b8ddc-ff10-4936-9fb1-617000000000/iec-23837-2>

| |
|--|
| Style Definition: Heading 1: Indent: Left: 0 pt, First line: 0 pt, Tab stops: Not at 21.6 pt |
| Style Definition: Heading 2: Font: Bold, Tab stops: Not at 18 pt |
| Style Definition: Heading 3: Font: Bold |
| Style Definition: Heading 4: Font: Bold |
| Style Definition: Heading 5: Font: Bold |
| Style Definition: Heading 6: Font: Bold |
| Style Definition: ANNEX |
| Style Definition: zzCopyright |
| Style Definition: AMEND Terms Heading: Font: Bold |
| Style Definition: AMEND Heading 1 Unnumbered: Font: Bold |
| Style Definition: Footnote Reference |
| Style Definition: Footnote Text |
| Style Definition: 井号标签1 |
| Style Definition: List Bullet: Indent: Left: 0 pt, Hanging: 18 pt, No bullets or numbering, Tab stops: 18 pt, List tab |
| Style Definition: List Bullet 3: Indent: Left: 28.3 pt, Hanging: 18 pt, No bullets or numbering, Tab stops: 46.3 pt, List tab |
| Style Definition: List Bullet 4: Indent: Left: 42.45 pt, Hanging: 18 pt, No bullets or numbering, Tab stops: 60.45 pt, List tab |
| Style Definition: List Bullet 5: Indent: Left: 56.6 pt, Hanging: 18 pt, No bullets or numbering, Tab stops: 74.6 pt, List tab |
| Style Definition: List Number: Indent: Left: 0 pt, Hanging: 18 pt, No bullets or numbering, Tab stops: 18 pt, List tab |
| Style Definition: List Number 5: Indent: Left: 56.6 pt, Hanging: 18 pt, No bullets or numbering, Tab stops: 74.6 pt, List tab |
| Style Definition: @他1 |
| Style Definition: 智能超链接1 |
| Style Definition: 未处理的提及2 |
| Style Definition: Unresolved Mention2 |
| Style Definition: IneraTableMultiPar: Font: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers, Tab stops: 19.85 pt, Left + 39.7 pt, Left + 59.55 pt, Left + 79.4 pt, Left + 99.25 pt, Left + 119.05 pt, Left + 138.9 pt, Left + 158.75 pt, Left + 178.6 pt, Left + 198.45 pt, Left |

Edited DIS - MUST BE USED FOR FINAL DRAFT

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC 23837-2

<https://standards.iteh.ai/catalog/standards/sist/654b8ddc-ff10-4936-9fb8-e06b64f43505/iso-iec-23837-2>

Edited DIS - MUST BE USED FOR FINAL DRAFT

© ISO 20222023

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~~ Copyright Office

CP 401 • ~~Ch. de Blandonnet 8~~

CH-1214 Vernier, Geneva

Phone: +41 22 749 01 11

Email: ~~copyright@iso.org~~

Email: ~~copyright@iso.org~~

Website: ~~www.iso.org~~ www.iso.org

Published in Switzerland.

Formatted: No page break before

Formatted: Default Paragraph Font

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC 23837-2

<https://standards.iteh.ai/catalog/standards/sist/654b8ddc-ff10-4936-9fb8-e06b64f43505/iso-iec-23837-2>

Edited DIS - MUST BE USED FOR FINAL DRAFT

Contents

| | |
|---|----|
| Foreword..... | v |
| Introduction..... | vi |
| 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..... | 7 |
| 5.3.3 — EAs for SFRs on quantum optical components and parameter adjustment procedure(s)..... | 7 |
| 5.3.4 — EAs for SFRs on conventional network components..... | 8 |
| 5.3.5 — Thresholds and input parameters related to the evaluation activities..... | 8 |
| 5.4 — Overview of evaluation activities for SARs..... | 9 |
| 6 — EAs for the evaluation of FTP_QKD..... | 9 |
| 6.1 — General..... | 9 |
| 6.2 — EA to test quantum state transmission and sifting procedures..... | 11 |
| 6.2.1 — General aspects..... | 11 |
| 6.2.2 — Test procedure..... | 14 |
| 6.2.3 — Pass/fail criteria..... | 16 |
| 6.3 — EA to test other post-processing procedures..... | 17 |
| 6.3.1 — General aspects..... | 17 |
| 6.3.2 — Test procedure..... | 19 |
| 6.3.3 — Pass/fail criteria..... | 20 |
| 6.4 — EA to test parameter adjustment procedure(s)..... | 20 |
| 6.4.1 — General aspects..... | 20 |
| 6.4.2 — Test procedure..... | 22 |
| 6.4.3 — Pass/fail criteria..... | 22 |
| 7 — EAs for evaluating quantum optical components in the transmitter module..... | 23 |
| 7.1 — General..... | 23 |
| 7.2 — EA to test the photon number distribution of optical pulses..... | 25 |
| 7.2.1 — General aspects..... | 25 |
| 7.2.2 — Test procedure..... | 28 |
| 7.2.3 — Pass/fail criteria..... | 30 |
| 7.3 — EA to test the mean photon number and stability of optical pulses..... | 30 |
| 7.3.1 — General aspects..... | 30 |
| 7.3.2 — Test procedure..... | 32 |
| 7.3.3 — Pass/fail criteria..... | 34 |
| 7.4 — EA to test the independence of the intensities of optical pulses..... | 34 |
| 7.4.1 — General aspects..... | 34 |
| 7.4.2 — Test procedure..... | 35 |
| 7.4.3 — Pass/fail criteria..... | 37 |

| | | |
|--------|---|----|
| 7.5 | EA to test the accuracy of state encoding | 37 |
| 7.5.1 | General aspects | 37 |
| 7.5.2 | Test procedure | 39 |
| 7.5.3 | Pass/fail criteria | 40 |
| 7.6 | EA to test the indistinguishability of encoded states | 40 |
| 7.6.1 | General aspects | 40 |
| 7.6.2 | Test procedure | 42 |
| 7.6.3 | Pass/fail criteria | 44 |
| 7.7 | EA to test the uniform distribution of the global phase of optical pulses | 45 |
| 7.7.1 | General aspects | 45 |
| 7.7.2 | Test procedure | 47 |
| 7.7.3 | Pass/fail criteria | 48 |
| 7.8 | EA to test the degree of optical isolation of the TX module | 48 |
| 7.8.1 | General aspects | 48 |
| 7.8.2 | Test procedure | 50 |
| 7.8.3 | Pass/fail criteria | 50 |
| 7.9 | EA to test the sensitivity of the injected light monitor in the TX module | 50 |
| 7.9.1 | General aspects | 50 |
| 7.9.2 | Test procedure | 52 |
| 7.9.3 | Pass/fail criteria | 53 |
| 7.10 | EA to test the robustness of the TX module against laser injection | 53 |
| 7.10.1 | General aspects | 53 |
| 7.10.2 | Test procedure | 56 |
| 7.10.3 | Pass/fail criteria | 59 |
| 8 | EAs for the evaluation of quantum optical components in the receiver module | 59 |
| 8.1 | General | 59 |
| 8.2 | EA to test the consistency of detection probability in the RX module | 62 |
| 8.2.1 | General aspects | 62 |
| 8.2.2 | Test procedure | 64 |
| 8.2.3 | Pass/fail criteria | 65 |
| 8.3 | EA to test information leakage of back flashes from the RX module | 65 |
| 8.3.1 | General aspects | 65 |
| 8.3.2 | Test procedure | 67 |
| 8.3.3 | Pass/fail criteria | 68 |
| 8.4 | EA to test the degree of optical isolation of the RX module | 68 |
| 8.4.1 | General aspects | 68 |
| 8.4.2 | Test procedure | 70 |
| 8.4.3 | Pass/fail criteria | 70 |
| 8.5 | EA to test the sensitivity of the injected light monitor in the RX module | 71 |
| 8.5.1 | General aspects | 71 |
| 8.5.2 | Test procedure | 72 |
| 8.5.3 | Pass/fail criteria | 73 |
| 8.6 | EA to test the robustness of the RX module against bright light blinding | 73 |
| 8.6.1 | General aspects | 73 |
| 8.6.2 | Test procedure | 75 |
| 8.6.3 | Pass/fail criteria | 77 |
| 8.7 | EA to test the appropriateness of dead time settings of SPDs | 77 |
| 8.7.1 | General aspect | 77 |
| 8.7.2 | Test procedure | 78 |
| 8.7.3 | Pass/fail criteria | 78 |
| 8.8 | EA to test the temporal profile of the detection efficiency for SPDs | 78 |

| | | |
|-----------------------|--|-----|
| 8.8.1 | General aspects | 78 |
| 8.8.2 | Test procedure | 80 |
| 8.8.3 | Pass/fail criteria | 81 |
| 8.9 | EA to test the robustness of the RX module against laser injection | 81 |
| 8.9.1 | General aspects | 81 |
| 8.9.2 | Test procedure | 83 |
| 8.9.3 | Pass/fail criteria | 85 |
| 8.10 | EA to test the detection limits of homodyne detectors in the RX module | 85 |
| 8.10.1 | General aspects | 85 |
| 8.10.2 | Test procedure | 86 |
| 8.10.3 | Pass/fail criteria | 87 |
| 8.11 | EA to test the appropriateness of double-click event handling | 87 |
| 8.11.1 | General aspects | 87 |
| 8.11.2 | Test procedure | 87 |
| 8.11.3 | Pass/fail criteria | 88 |
| 9 | EAs for the evaluation of parameter adjustment procedure(s) | 88 |
| 9.1 | General | 88 |
| 9.2 | EA to test the inducibility of detection probability mismatch | 88 |
| 9.2.1 | General aspects | 88 |
| 9.2.2 | Test procedure | 92 |
| 9.2.3 | Pass/fail criteria | 94 |
| 9.3 | EA to test the correctness of shot noise alignment | 95 |
| 9.3.1 | General aspects | 95 |
| 9.3.2 | Test procedure | 96 |
| 9.3.3 | pass/fail criteria | 99 |
| 10 | Supplementary activities for the evaluation of SFRs on conventional network components | 99 |
| 10.1 | General | 99 |
| 10.2 | Evaluation activities for FCS related SFRs overview | 100 |
| 10.3 | Evaluation activities for other SFRs overview | 100 |
| 11 | Supplementary activities for SARs | 100 |
| 11.1 | General | 100 |
| 11.2 | Supplementary activities for Class APE: Protection Profile evaluation | 101 |
| 11.3 | Supplementary activities for Class ASE: Security Target evaluation | 102 |
| 11.4 | Supplementary activities for Class ADV: Development | 103 |
| 11.4.1 | Supplementary activities for ADV_ARC | 103 |
| 11.4.2 | Supplementary activities for ADV_FSP | 104 |
| 11.5 | Supplementary activities for Class AGD: Guidance documents | 105 |
| 11.5.1 | Supplementary activities for AGD_OPE | 105 |
| 11.5.2 | Supplementary activities for AGD_PRE | 106 |
| 11.6 | Supplementary activities for Class ATE: Test | 106 |
| 11.6.1 | Supplementary activities for ATE_FUN | 106 |
| 11.6.2 | Supplementary activities for ATE_IND | 107 |
| 11.7 | Supplementary activities for Class AVA: Vulnerability assessment | 108 |
| 12 | Conformance statement | 111 |
| 12.1 | General | 111 |
| 12.2 | Conformance statement specific to evaluation activities for SFRs | 111 |
| 12.3 | Conformance statement specific to EAs for SARs | 112 |
| Annex A (informative) | Guidance on the calculation of attack potential for the evaluation of QKD modules | 113 |

| | | |
|--------------|--|-------------|
| A.1 | General | 113 |
| A.2 | Identification and exploitation of attacks | 113 |
| A.2.1 | General | 113 |
| A.2.2 | Identification of attacks | 113 |
| A.2.3 | Exploitation of attacks | 114 |
| A.3 | Factors for attack potential calculation | 114 |
| A.3.1 | General | 114 |
| A.3.2 | Elapsed time | 114 |
| A.3.3 | Expertise | 115 |
| A.3.4 | Knowledge of the TOE | 116 |
| A.3.5 | Window of opportunity | 116 |
| A.3.6 | Equipment | 117 |
| A.4 | Calculation of attack potential | 117 |
| | Annex B (informative) Rating examples for AVA attack potential computation | 121 |
| B.1 | General | 121 |
| B.2 | Example 1 – Trojan horse attack | 121 |
| B.3 | Example 2 – Wavelength attack | 122 |
| | Annex C (informative) Thresholds collection | 124 |
| | Annex D (informative) Correspondence between EAs and known attacks to quantum optical components and parameter adjustment procedure(s) of QKD modules | 129 |
| | Bibliography | 131 |
| | Foreword | vii |
| | Introduction | viii |
| 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 | 7 |
| 5.3.3 | EAs for SFRs on quantum optical components and parameter adjustment procedure(s) | 7 |
| 5.3.4 | EAs for SFRs on conventional network components | 8 |
| 5.3.5 | Thresholds and input parameters related to the evaluation activities | 8 |
| 5.4 | Overview of evaluation activities for SARs | 9 |
| 6 | EAs for the evaluation of FTP_QKD | 9 |

| | | |
|--------|--|----|
| 6.1 | General..... | 9 |
| 6.2 | EA to test quantum state transmission and sifting procedures..... | 11 |
| 6.2.1 | General aspects..... | 11 |
| 6.2.2 | Test procedure..... | 14 |
| 6.2.3 | Pass/fail criteria..... | 16 |
| 6.3 | EA to test other post-processing procedures..... | 17 |
| 6.3.1 | General aspects..... | 17 |
| 6.3.2 | Test procedure..... | 19 |
| 6.3.3 | Pass/fail criteria..... | 20 |
| 6.4 | EA to test parameter adjustment procedure(s)..... | 20 |
| 6.4.1 | General aspects..... | 20 |
| 6.4.2 | Test procedure..... | 22 |
| 6.4.3 | Pass/fail criteria..... | 22 |
| 7 | EAs for evaluating quantum optical components in the transmitter module..... | 23 |
| 7.1 | General..... | 23 |
| 7.2 | EA to test the photon-number distribution of optical pulses..... | 25 |
| 7.2.1 | General aspects..... | 25 |
| 7.2.2 | Test procedure..... | 28 |
| 7.2.3 | Pass/fail criteria..... | 30 |
| 7.3 | EA to test the mean photon number and stability of optical pulses..... | 30 |
| 7.3.1 | General aspects..... | 30 |
| 7.3.2 | Test procedure..... | 32 |
| 7.3.3 | Pass/fail criteria..... | 34 |
| 7.4 | EA to test the independence of the intensities of optical pulses..... | 34 |
| 7.4.1 | General aspects..... | 34 |
| 7.4.2 | Test procedure..... | 35 |
| 7.4.3 | Pass/fail criteria..... | 37 |
| 7.5 | EA to test the accuracy of state encoding..... | 37 |
| 7.5.1 | General aspects..... | 37 |
| 7.5.2 | Test procedure..... | 39 |
| 7.5.3 | Pass/fail criteria..... | 40 |
| 7.6 | EA to test the indistinguishability of encoded states..... | 40 |
| 7.6.1 | General aspects..... | 40 |
| 7.6.2 | Test procedure..... | 42 |
| 7.6.3 | Pass/fail criteria..... | 44 |
| 7.7 | EA to test the uniform distribution of the global phase of optical pulses..... | 45 |
| 7.7.1 | General aspects..... | 45 |
| 7.7.2 | Test procedure..... | 47 |
| 7.7.3 | Pass/fail criteria..... | 48 |
| 7.8 | EA to test the degree of optical isolation of the TX module..... | 48 |
| 7.8.1 | General aspects..... | 48 |
| 7.8.2 | Test procedure..... | 50 |
| 7.8.3 | Pass/fail criteria..... | 50 |
| 7.9 | EA to test the sensitivity of the injected light monitor in the TX module..... | 50 |
| 7.9.1 | General aspects..... | 50 |
| 7.9.2 | Test procedure..... | 52 |
| 7.9.3 | Pass/fail criteria..... | 53 |
| 7.10 | EA to test the robustness of the TX module against laser injection..... | 53 |
| 7.10.1 | General aspects..... | 53 |
| 7.10.2 | Test procedure..... | 56 |
| 7.10.3 | Pass/fail criteria..... | 59 |

REVIEW
ai)
standards.ieb.ai/catalog/standards/sist/654b84dc-04936-9fb8-e06b64f43505/iso-

| | | |
|----------|--|-----------|
| 8 | EAs for the evaluation of quantum optical components in the receiver module | 59 |
| 8.1 | General | 59 |
| 8.2 | EA to test the consistency of detection probability in the RX module | 62 |
| 8.2.1 | General aspects | 62 |
| 8.2.2 | Test procedure | 64 |
| 8.2.3 | Pass/fail criteria | 65 |
| 8.3 | EA to test information leakage of back-flashes from the RX module | 65 |
| 8.3.1 | General aspects | 65 |
| 8.3.2 | Test procedure | 67 |
| 8.3.3 | Pass/fail criteria | 68 |
| 8.4 | EA to test the degree of optical isolation of the RX module | 68 |
| 8.4.1 | General aspects | 68 |
| 8.4.2 | Test procedure | 70 |
| 8.4.3 | Pass/fail criteria | 70 |
| 8.5 | EA to test the sensitivity of the injected light monitor in the RX module | 71 |
| 8.5.1 | General aspects | 71 |
| 8.5.2 | Test procedure | 72 |
| 8.5.3 | Pass/fail criteria | 73 |
| 8.6 | EA to test the robustness of the RX module against bright light blinding | 73 |
| 8.6.1 | General aspects | 73 |
| 8.6.2 | Test procedure | 75 |
| 8.6.3 | Pass/fail criteria | 77 |
| 8.7 | EA to test the appropriateness of dead time settings of SPDs | 77 |
| 8.7.1 | General aspect | 77 |
| 8.7.2 | Test procedure | 78 |
| 8.7.3 | Pass/fail criteria | 78 |
| 8.8 | EA to test the temporal profile of the detection efficiency for SPDs | 78 |
| 8.8.1 | General aspects | 78 |
| 8.8.2 | Test procedure | 80 |
| 8.8.3 | Pass/fail criteria | 81 |
| 8.9 | EA to test the robustness of the RX module against laser injection | 81 |
| 8.9.1 | General aspects | 81 |
| 8.9.2 | Test procedure | 83 |
| 8.9.3 | Pass/fail criteria | 85 |
| 8.10 | EA to test the detection limits of homodyne detectors in the RX module | 85 |
| 8.10.1 | General aspects | 85 |
| 8.10.2 | Test procedure | 86 |
| 8.10.3 | Pass/fail criteria | 87 |
| 8.11 | EA to test the appropriateness of double-click event handling | 87 |
| 8.11.1 | General aspects | 87 |
| 8.11.2 | Test procedure | 87 |
| 8.11.3 | Pass/fail criteria | 88 |
| 9 | EAs for the evaluation of parameter adjustment procedure(s) | 88 |
| 9.1 | General | 88 |
| 9.2 | EA to test the inducibility of detection probability mismatch | 88 |
| 9.2.1 | General aspects | 88 |
| 9.2.2 | Test procedure | 92 |
| 9.2.3 | Pass/fail criteria | 94 |
| 9.3 | EA to test the correctness of shot noise alignment | 95 |
| 9.3.1 | General aspects | 95 |
| 9.3.2 | Test procedure | 96 |

| | | |
|-----------------------|--|-----|
| 9.3.3 | pass/fail criteria | 99 |
| 10 | Supplementary activities for the evaluation of SFRs on conventional network components | 99 |
| 10.1 | General..... | 99 |
| 10.2 | Evaluation activities for FCS related SFRs overview | 100 |
| 10.3 | Evaluation activities for other SFRs overview..... | 100 |
| 11 | Supplementary activities for SARs..... | 100 |
| 11.1 | General..... | 100 |
| 11.2 | Supplementary activities for class APE: Protection profile evaluation..... | 101 |
| 11.3 | Supplementary activities for class ASE: Security target evaluation | 102 |
| 11.4 | Supplementary activities for Class ADV: Development..... | 103 |
| 11.4.1 | Supplementary activities for ADV ARC..... | 103 |
| 11.4.2 | Supplementary activities for ADV FSP | 104 |
| 11.5 | Supplementary activities for Class AGD: Guidance documents | 105 |
| 11.5.1 | Supplementary activities for AGD OPE..... | 105 |
| 11.5.2 | Supplementary activities for AGD PRE..... | 106 |
| 11.6 | Supplementary activities for Class ATE: Test | 106 |
| 11.6.1 | Supplementary activities for ATE FUN | 106 |
| 11.6.2 | Supplementary activities for ATE IND..... | 107 |
| 11.7 | Supplementary activities for Class AVA: Vulnerability assessment..... | 108 |
| 12 | Conformance statement | 111 |
| 12.1 | General..... | 111 |
| 12.2 | Conformance statement specific to evaluation activities for SFRs | 111 |
| 12.3 | Conformance statement specific to EAs for SARs | 112 |
| Annex A (informative) | Guidance on the calculation of attack potential for the evaluation of QKD modules..... | 113 |
| A.1 | General..... | 113 |
| A.2 | Identification and exploitation of attacks..... | 113 |
| A.2.1 | General..... | 113 |
| A.2.2 | Identification of attacks..... | 113 |
| A.2.3 | Exploitation of attacks | 114 |
| A.3 | Factors for attack potential calculation | 114 |
| A.3.1 | General..... | 114 |
| A.3.2 | Elapsed time..... | 114 |
| A.3.3 | Expertise..... | 115 |
| A.3.4 | Knowledge of the TOE | 116 |
| A.3.5 | Window of opportunity | 116 |
| A.3.6 | Equipment..... | 117 |
| A.4 | Calculation of attack potential..... | 117 |
| Annex B (informative) | Rating examples for AVA attack potential computation | 121 |
| B.1 | General..... | 121 |
| B.2 | Example 1 – Trojan horse attack | 121 |

STANDARD PREVIEW

ISO/IEC 23837-2

<https://standards.iso.org/standards/catalog/standards/sist/65468ddc-110-4936-9fb8-e06b64f43505/iso-iec-23837-2>

| | |
|--|------------|
| B.3 Example 2 – Wavelength attack | 122 |
| Annex C (informative) Thresholds collection | 124 |
| Annex D (informative) Correspondence between EAs and known attacks to quantum optical components and parameter adjustment procedure(s) of QKD modules | 129 |
| Bibliography | 131 |

Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC 23837-2

<https://standards.iteh.ai/catalog/standards/sist/654b8ddc-ff10-4936-9fb8-e06b64f43505/iso-iec-23837-2>

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.

Formatted: English (United Kingdom)

Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

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).

Formatted: Indent: Left 0 ch, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: English (United Kingdom)

Formatted: English (United Kingdom)

Attention is drawn to the possibility that some of the elements implementation of this document may be involved in the subject 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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see <https://patents.iec.ch>).

Formatted: English (United Kingdom)

Formatted: English (United Kingdom)

Formatted: English (United Kingdom)

Formatted: English (United Kingdom)

Formatted: English (United Kingdom)

Formatted: English (United Kingdom)

Formatted: English (United Kingdom)

Formatted: English (United Kingdom)

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.

Formatted: English (United Kingdom)

Formatted: English (United Kingdom)

Formatted: English (United Kingdom)

Formatted: std_publisher, English (United Kingdom)

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, Information technology, Subcommittee SC-27, Information security, cybersecurity and privacy protection.

Formatted: English (United Kingdom)

Formatted: std_docNumber, English (United Kingdom)

A list of all parts in the ISO/IEC 23837 series can be found on the ISO website.

Formatted: English (United Kingdom)

Formatted: Font: Not Italic

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.

Formatted: English (United Kingdom)

Formatted: std_publisher

Formatted: std_docNumber

Formatted: std_docPartNumber

Formatted: English (United Kingdom)

Formatted: Foreword Text, Indent: Left 0 ch, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: English (United Kingdom)

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.

Formatted: Default Paragraph Font

Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: std_docPartNumber

ITEH STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC 23837-2

<https://standards.iteh.ai/catalog/standards/sist/654b8ddc-ff10-4936-9fb8-e06b64f43505/iso-iec-23837-2>