ISO/IEC DIS 23837-~~-~~2:~~2022~~2023(E)

ISO/IEC JTC 1/SC 27/WG 3

Date: 2023-~~01-12~~06-20

Information security — Security requirements, test and evaluation methods for quantum key distribution — Part 2: ~~Test~~Evaluation and ~~evaluation~~testing methods

~~Edited DIS - MUST BE USED FOR FINAL DRAFT~~

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

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

Edited DIS - MUST BE USED FOR FINAL DRAFT

Formatted: No page break before

Formatted: Default Paragraph Font

Contents

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

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~~www.iso.org/directives or ~~www.iec.ch/members_experts/refdocs~~www.iec.ch/members_experts/refdocs).

~~Attention is drawn~~ISO and IEC draw attention to the possibility that ~~some of~~the ~~elements~~implementation of this document may ~~be~~involve the ~~subject~~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. ~~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).~~

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~~ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see ~~www.iso.org/iso/foreword.html~~www.iso.org/iso/foreword.html. In the IEC, see ~~www.iec.ch/understanding-standards~~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~~www.iso.org/members.html and www.iec.ch/national-committees.

Formatted: English (United Kingdom)
Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
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)
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)
Formatted: English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: std_publisher, English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: std_docNumber, English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: Font: Not Italic
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