INTERNATIONAL STANDARD

ISO/IEC 23837-1

First edition
2023-08

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

Part 1: **Requirements**

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

Partie 1: Exigences

Reference number
ISO/IEC 23837-1:2023(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword v

Introduction vi

1 Scope 1

2 Normative references 1

3 Terms and definitions 1

4 Abbreviated terms 5

5 Theoretical aspects of QKD protocols 6
5.1 General 6
5.2 Principle 6
5.3 Classification 7
5.4 Architecture 8

6 Implementation modules of QKD protocols 10
6.1 General 10
6.2 External interfaces of QKD modules 11
6.2.1 General 11
6.2.2 The quantum channel interface 11
6.2.3 The control and management interface 11
6.2.4 The key management interface 12
6.3 Internal structure of QKD modules 12
6.3.1 General 12
6.3.2 Components in the QKD transmitter module 13
6.3.3 Components in the QKD receiver module 15
6.4 TOE scope for QKD modules 15
6.4.1 General 15
6.4.2 Definition of the TSF 15
6.4.3 Definition of the TOE 16
6.5 General working flow of QKD modules 17

7 Security problems analysis of QKD modules 17
7.1 General 17
7.2 Security assumptions 17
7.3 Assets analysis 19
7.4 Threats to conventional network components 19
7.4.1 Overview 19
7.4.2 Threats from the perspective of network-based classical attacks 20
7.5 Threats to quantum optical components 22
7.5.1 Overview 22
7.5.2 Threats exploiting optical source flaws 22
7.5.3 Threats exploiting optical detection vulnerabilities 22
7.5.4 Threats exploiting parameter adjustment vulnerabilities 22

8 Extended security functional components for QKD implementation 23
8.1 General 23
8.2 Extended security functional components to Class FTP: Trusted path/channels 23
8.2.1 Quantum key distribution (FTP_QKD) 23
8.2.2 User notes 27

9 Security functional requirements for QKD modules 29
9.1 General 29
9.2 General requirements for conventional network components in QKD modules 31
9.2.1 FAU_GEN.1 Audit data generation 31
9.2.2 FCS_CKM.6 Timing and event of cryptographic key destruction 31
9.2.3 FCS_COP.1 Cryptographic operation 32
9.2.4 FCS_RNG.1 Random number generation 33