

ISO/IEC 23837-1:2023-08 (E)

Information security - Security requirements, test and evaluation methods for quantum key distribution - Part 1: Requirements

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
9.2.5	FDP_ACC.1 Subset access control.....	33
9.2.6	FDP_ACF.1 Security attribute-based access control.....	34
9.2.7	FDP_IRC.1 Information retention control.....	34
9.2.8	FDP_ITC.1 Import of user data without security attributes.....	35
9.2.9	FIA_UAU.2 User authentication before any action.....	36
9.2.10	FIA_UID.1 Timing of identification.....	36
9.2.11	FMT_LIM.1 Limited capabilities.....	36
9.2.12	FMT_LIM.2 Limited availability.....	37
9.2.13	FMT_MSA.1 Management of security attributes.....	37
9.2.14	FMT_MTD.1 Management of TSF data.....	37
9.2.15	FMT_SMF.1 Specification of management functions.....	38
9.2.16	FMT_SMR.1 Security roles.....	38
9.2.17	FPT_EMS.1/Convention Emanation of TSF and User data.....	39
9.2.18	FPT_FLS.1 Failure with preservation of secure state.....	39
9.2.19	FPT_ITC.1 Inter-TSF confidentiality during transmission.....	40
9.2.20	FPT_ITI.1 Inter-TSF detection of modification.....	40
9.2.21	FPT_RCV.2 Automated recovery.....	41
9.2.22	FPT_TST.1 TSF self-testing.....	42
9.3	General requirements for the implementation of QKD protocols.....	43
9.3.1	General.....	43
9.3.2	FPT_QKD.1 QKD protocol and raw data generation.....	43
9.3.3	FPT_QKD.2 QKD post-processing.....	44
9.4	General requirements for quantum optical components of QKD modules.....	44
9.4.1	General.....	44
9.4.2	FPT_EMS.1/Quantum emanation of TSF and user data.....	45
9.4.3	FPT_PHP.3 Resistance to physical attack.....	45
10	Conformance statement.....	47
10.1	General.....	47
10.2	Conformance statement specific to the security problem definition.....	47
10.3	Conformance statement specific to the security functional requirements.....	48
Annex A (informative) Guidance for developing protection profiles for QKD modules.....		49
Bibliography.....		52