परीक्षण निर्देशिका
टीईसी ९१०००:२०२६
(सं. टीईसी ९१०००१:२०२३ को अधिक्रमित करता है)

TEST GUIDE
TEC 91001:2026
(Supersedes No. TEC 91001:2023)

for

क्वांटम कुंजी वितरण प्रणाली
Quantum Key Distribution System
(TEC 91000:2026)

ISO 9001:2015

दूरसंचार अभियांत्रिकी केंद्र
खुर्शीदलाल भवन, जनपथ, नई दिल्ली-110001,भारत
TELECOMMUNICATION ENGINEERING CENTRE
KHURSHID LAL BHAWAN, JANPATH, NEW DELHI-110001, INDIA
www.tec.gov.in

Draft Release 2: June, 2026

FOREWORD

Telecommunication Engineering Centre (TEC) is the technical arm of Department of Telecommunications (DOT), Government of India. Its activities include:

- Framing of TEC Standards for Generic Requirements for a Product/Equipment, Standards for Interface Requirements for a Product/Equipment, Standards for Service Requirements & Standard document of TEC for Telecom Products and Services
- Formulation of Essential Requirements (ERs) under Mandatory Testing and Certification of Telecom Equipment (MTCTE)
- Field evaluation of Telecom Products and Systems
- Designation of Conformity Assessment Bodies (CABs)/Testing facilities
- Testing & Certification of Telecom products
- Adoption of Standards
- Support to DoT on technical/technology issues

For the purpose of testing, four Regional Telecom Engineering Centers (RTECs) have been established which are located at New Delhi, Bangalore, Mumbai, and Kolkata.

ABSTRACT

This Test Guide of testing pertains to detailed provisional test schedule and test procedure for evaluating conformance/functionality/requirements/ performance of standard on Quantum Key Distribution System as per standard no. TEC 91000:2026.

CONTENTS

A. HISTORY SHEET

Sl.No.	*Standard/document No.*	*Title*	*Remarks*
1.	TEC 91001:2022	Test Guide for Quantum Key Distribution (QKD) System	First Issue March, 2023
2.	TEC 91001:2026	Test Guide for Quantum Key Distribution (QKD) System	Second Issue ____, 2026

B. INTRODUCTION

This document describes the test schedule and procedures for evaluating the requirements of functionality / performance / operational / interface / interoperability / quality / safety / Electromagnetic compatibility, security services and performance under the Standard on Quantum Key Distribution System against the Generic requirements as per the TEC GR No.: TEC 91000:2026.

The manufacturer shall offer the system for type evaluation along with the following documents:

i. System specifications of the equipment containing features, facilities, and physical description,
ii. Installation, System and Operation & Maintenance manual of the equipment,
iii. Hardware, Software, and firmware details of the equipment,
iv. Bill of material,
v. Block schematic diagram and physical configuration of the equipment,
vi. Test Results as per the TEC Test Guide for the GR.

All the necessary set-ups & measuring instruments duly calibrated by an authorised lab shall be provided by the manufacturer for testing. The manufacturer shall provide proper operating environment required for testing.

Note: Though every care has been taken to cover all the parameters of the GR correctly in this Test Guide, yet to avoid any inadvertent error/ misprint, the testing officer shall ensure that all the parameters of the GR have been tested & verified in accordance with the provisions of the GR, same will be reflected on the report.

C. General Information

Sn	General Information	Details (to be filled by testing team)			
1.	Name and Address of the Applicant				
2.	Date of Registration				
3.	Name and No. of TEC Standard /Applicant's Spec. against which the approval sought				
4.	Topology of QKD System offered for testing	P2P QKD without Relay Nodes	P2P QKD with Relay nodes	Point to Multi-Point Topology / Star Topology	Multi-point QKD Topology
5.	Type of product	Short Range	Long Range	Extended Range	
6.	Details of Equipment				
	Type of the Equipment	Model No.		Serial No.	
(i)					
(ii)					
(iii)					

7.	Date of commencement of Tests		
8.	Place of Testing		
9.	QKD Protocol(s) supported		
10.	Any other relevant information:-		

D. Testing team

S. no.	Name	Designation	Organization	Signature
1.				
2.				

E. List of the test instruments:

S. no.	Name of the test instrument	Make/Model *(to be filled by team)*	Validity of calibration *(to be filled by testing team)*
1.			_ _/_ _/_ _ _
2.			
3.			
4.			
5.			
6.			
7.			
8.			

F. Equipment Configuration Offered:

a) ..... Configuration

S. No.	Item	Details	Remarks

Relevant information like No. of cards, ports, slots, interfaces, size etc. may be filled as applicable for the product

b) ..... Configuration

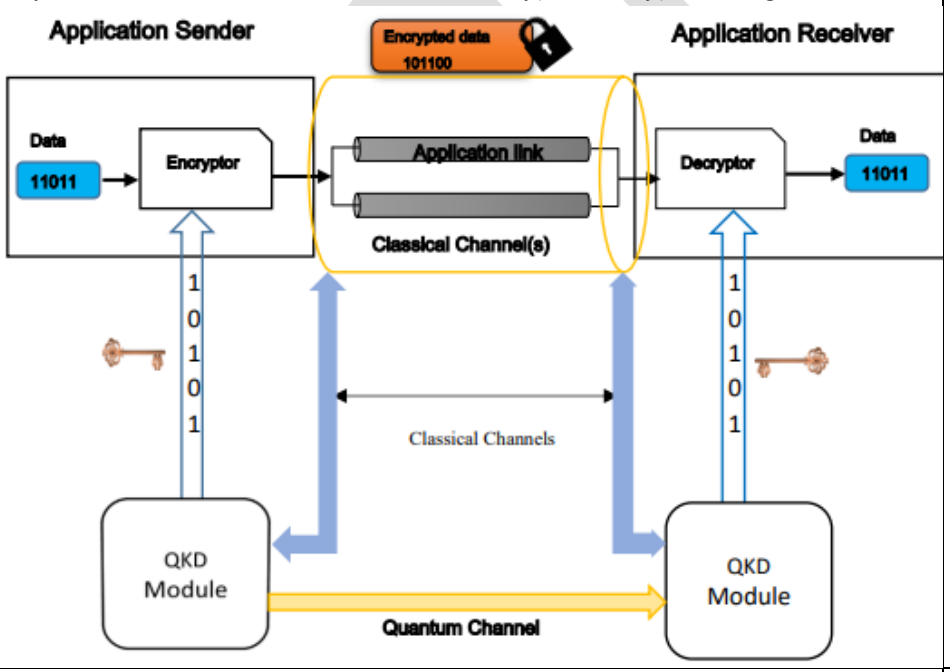
S. No.	Item	Details	Remarks

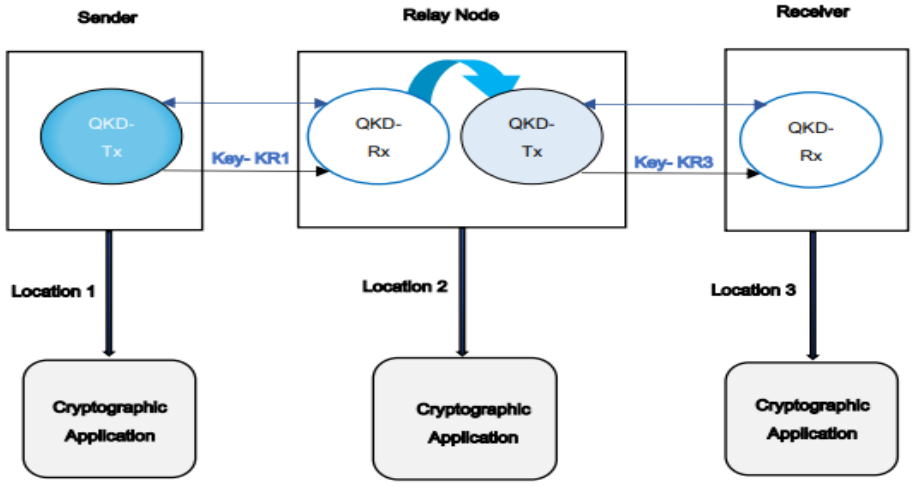
Relevant information like No. of cards, ports, slots, interfaces, size etc. may be filled as applicable for the product

G. Equipment/System Manuals:

*Availability of Maintenance manuals, Installation manual, Repair manual & User Manual etc. (**Y/N**)*

H. Clause-wise Test Type and Test No.:

Clause No.	Clause	Type of Test/Test No. etc.
	CHAPTER 1	
1.1	Introduction to QKD technology	
	This document describes the generic requirements and specifications for Quantum Key Distribution (QKD) system for use in the Indian telecom network. This document covers QKD protocols under distributed phase reference protocols like Coherent One Way (COW), Differential Phase Shift (DPS), etc. The other protocols and Wave Division Multiplexing (WDM) based QKD systems will be covered in the next issue.	This is for information purpose.
1.1.1	A Quantum Key Distribution (QKD) system is a secure communication method which implements a cryptographic protocol involving the principles of quantum mechanics. It enables two parties to produce a shared random secret key known only to them, which can then be used to encrypt & decrypt messages.  	This is for information purpose.
1.1.2	The basic elements of a P2P QKD system are a transmitter (QKD-Tx) and a receiver (QKD-Rx), each of which is referred to as a QKD module. A QKD link connects the QKD modules directly or with the help of a quantum relay point. Initial communication of raw keys is shared through Quantum links. The QKD link usually consists of a quantum channel and a classical channel(s). The quantum channel may be reserved for quantum signals, such as a single-photon-level coherent state of light to transmit random bit strings. The classical channel(s) is	This is for information purpose.

	mainly reserved for synchronization and may be for data exchange between the QKD modules or data exchange via existing IP network infrastructure, if required. Figure 1 illustrates an example of applying QKD to secure a point-to-point (P-to-P) application link. QKD modules generate keys and supply them to the applications. The application link where encrypted data is transmitted can be any communication link in a conventional or a future network. The QKD link usually consists of a quantum channel and a classical channel(s). Therefore, QKD is an add-on technology (and service) to existing or future networks. Information theoretical security of QKD is guaranteed by the laws of quantum mechanics and quantum information theory. QKD module shall have a tamper detection feature.	
1.1.3	P2P QKD System with Relay Node	
	In real applications, QKD links are limited to around 80-100KM without a relay in optical fibres. As of now, Quantum Repeaters, Quantum Memories, etc. are limited in practical implementation. Hence, the QKD relay nodes are one of the effective solutions to extend the range of the QKD system. In this type of QKD system, a QKD key Relay Node Module is used for Key Relaying. Relay nodes not only extend the coverage of QKD links but also help to handle point-to-multipoint (P2MP) quantum networks. They are intrinsically desirable for urban and access networks with mesh, star or tree topologies where the relay nodes are located at hubs where quantum receivers are centralized and shared by multiple users. To add a new node, only lasers, electronic systems and modulators are needed at the relay node. Relatively a few additional hardware requirements make relaying networks scalable for a large number of users.  Figure 2 P2P QKD System with Relay Node The operating principle of the trusted relay P2P QKD system shown above is explained below.	This is for information purpose.

	Assuming that earlier a pair of QKD Modules (Sender at Location 1 and Receiver at Location 3) were connected directly (point to point) by the QKD link. Now a QKD relay node (R) is added at an intermediate location for Key Relaying. Location '1' and Location '2' generating key 'KR1', Location '2' and Location '3' generating key 'KR3'. Such QKD keys can be directly used to secure communication respectively between Location 1 & 2, Location 2 & 3. Now, an information theoretic secure mathematical function/algorithm shall be used to securely relay the Key at the intermediate office by using both KR1 and KR3 so that Location '1' and Location '3' will have the same key. These keys can be used for securing communication between Locations 1 and 3. The relay node may be implemented either as a single integrated solution that includes provisions for both Alice and Bob functionalities within one physical unit, or as a two-unit solution comprising separate Alice and Bob units housed in distinct enclosures. Also in a network architecture, the relay node may be configured as an edge node.	
1.1.4	Network Topologies for QKD System: i. Star Topology [Point to Multi-Point Topology]: In QKD, the single-photon detector(s) are located in Bob (receiver) nodes and contribute to the majority of the cost for a QKD link. In order to save cost and serve areas where nodes are connected with a central node, Star type of QKD network topology can be used. Within a star topology, the system may be deployed in one of the following two configurations: The Star Topology may also be referred to as "Hub and Spoke" Topology. Single Star Configuration: In this setup, no redundancy is provided for the central node. Failure of the central node results in loss of connectivity between all connected end nodes.	This is for information purpose.

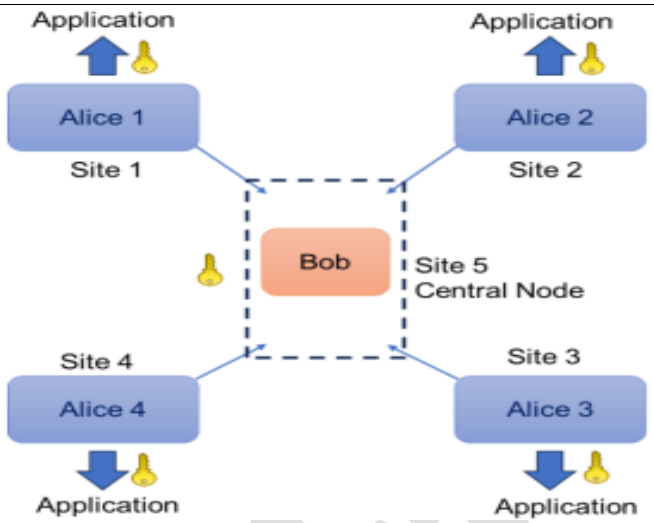


Figure 3A: Star QKD network topology

Fail-safe Dual Star Configuration:

This setup incorporates redundancy for the central node. In case of failure of the active central node, the system shall automatically switch to a standby (redundant) central node to maintain uninterrupted operation.

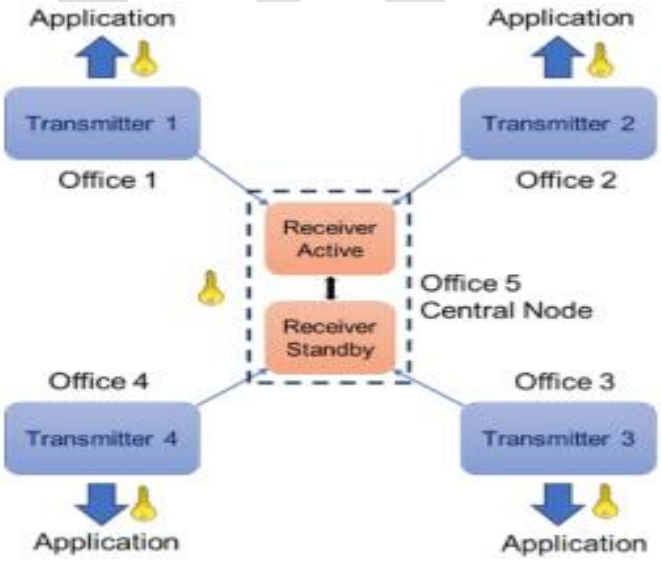
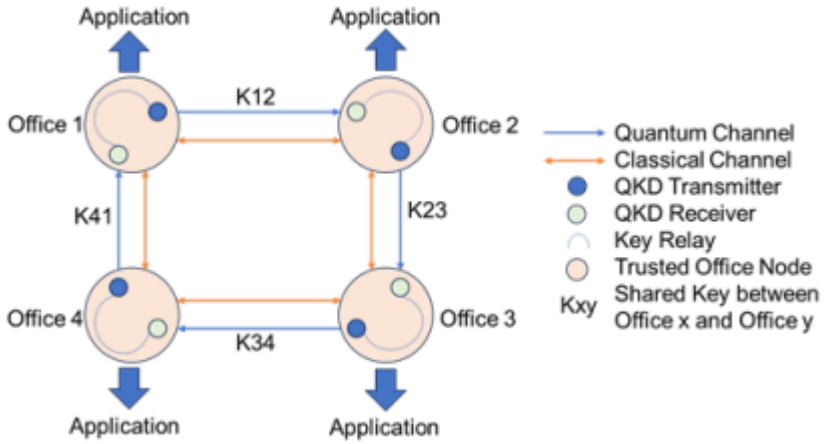
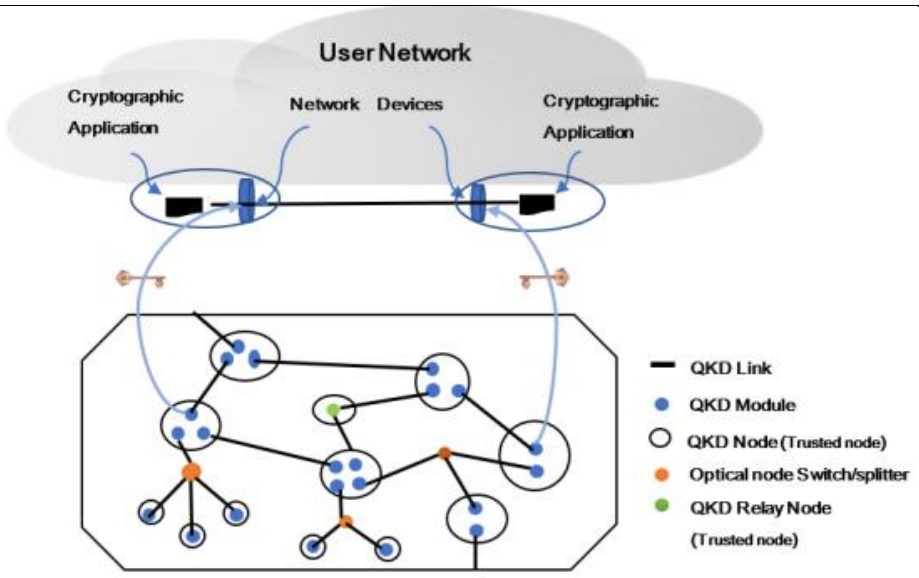


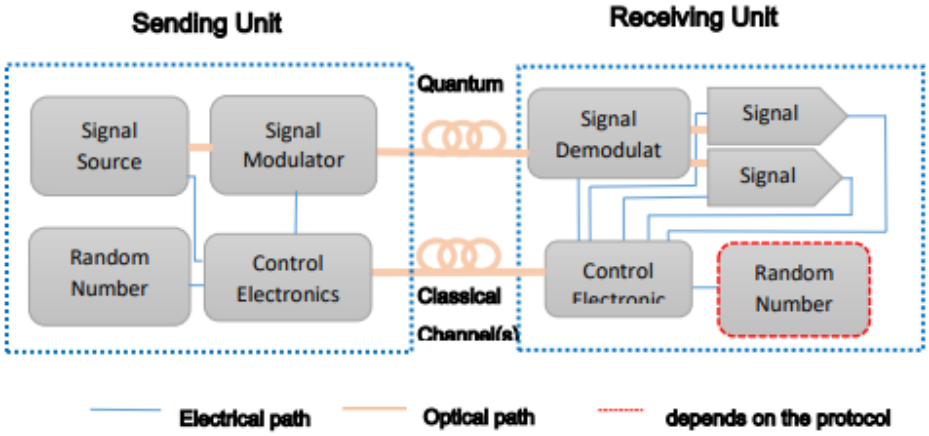
Figure 3B: Failsafe dual-star QKD network topology

ii. Ring Topology [Multi-point QKD Topology]:

Using the concept of trusted relay, ring topology can be used. This can address denial of service due to fibre cuts. As depicted in Figure below with 4 sites, the nodes can generate keys either clockwise or anti-clockwise using the trusted relay. For example, Office 1 and Office 2 are

	directly connected using a QKD link. In case of a fibre cut between them, these two offices can generate secure keys by using trusted relays at Office 4 and Office 3. Even if a fiber cut happens between any 02 pair of nodes, QKDN shall provide keys to cryptographic applications through alternate relayed path.  Figure 3C: QKD Ring network topology	
1.1.5	In a multipoint QKD deployment (Figure 4), secret keys are shared between any two parties in a user network and the range may also get extended to cater to a large network. As shown in figure 4, intermediate trusted nodes are mostly used for constructing a Multipoint QKD Network for increasing the range. These intermediate nodes securely relay the key generated in one QKD span over the next QKD span to ensure the availability of secure keys between any pair of encryption entities which might be seeking the keys. Figure 4 also illustrates the option of using optical switching/splitting for interconnecting one QKD node with more than one QKD node in a timeshared manner for optimally realising a QKD Network. Optical switches or splitters can switch or split QKD link traffic between pairs of QKD modules in the multi-point network to form keys between different users on demand. In addition to this, figure 4 depicts Quantum relay nodes which may evolve in future and can replace trusted nodes for extending the range in a QKD Network. In this scheme, keys are stored in QKD nodes (trusted nodes) and relayed to other distant QKD nodes with highly secure encryption. Currently, this is widely adopted for long-range QKD fibre networks secure.	This is for information purpose.

	 Figure 4 Multipoint QKD System	
1.1.6	The GR outlines the general characteristics of QKD systems including technical requirements for P2P and Multipoint QKD Systems.	This is for information purpose.
1.2	QKD System Architecture	
1.2.1	A QKD System shall consist of Sender & Receiver units which should be physically separated at opposite ends of a pair of a communication channel(s) that is a quantum and classical channel(s) as illustrated in figure 4. The Sender (Transmitter) and Receiver unit shall contain a source of randomness (depending upon the protocol) for use in the key generation protocol. The source of randomness shall be either a True random number generator or a Quantum random number generator. The Sender unit shall consist of a Coherent weak signal source or a single photon source. The encoder shall provide the qubit information including controlling the phase/time-bin or the discrete variable state of the transmitted photon. The Receiver unit should contain a component for signal detection, i.e., for selecting the measurement basis, as well as one or more signal detectors. Control electronics shall be used to generate the drive signals for these devices. The detected signals shall be used by the control electronics to form the initial (or raw) key, which shall then be post-processed (sifted, reconciled and privacy amplified) to achieve the final secure shared key.	This is for information purpose.

	 Figure 5 QKD System Architecture The Sender shall transmit qubit information to Receiver. Sender and Receiver shall exchange classical optical signals for clock synchronization/recovery, sifting and key post-processing. All communication shall be authenticated as per ISO 23837. The Classical channel can be implemented on a separate fibre or existing fibre carrying user traffic using Wavelength Division Multiplexing (WDM).	
1.3	QKD System Description	
1.3.1	QKD System Shall provide the following functionalities i. Interface from/to user /application interface ii. Key sifting, error estimation/correction and privacy amplification. iii. Key management. iv. Performance monitoring, system configuration and administration, auto calibration, system health parameters, etc.	Test Case No. 1
1.4	QKD Terminal Blocks	
1.4.1	Sender Node The Sender unit shall consist of a Coherent weak signal source or single photon source. The Sender unit shall be 19" rack-mountable with the height of size 1U/2U/3U, etc. It shall have provision for signal Source (Continuous wave laser/pulsed laser/ single photon source), modulation units (Intensity/Phase modulators), random number generator and control electronics system. For a single photon source, the second-order correlation value g2(0) shall be <<1 and mentioned in the product datasheet. For a weak coherent source, the second-order correlation value g2(0) shall be ~1.	Test Case No. 2
1.4.2	Receiver Node The Receiver's unit shall be a 19" rack-mountable with a height of size 1U/2U/3U, etc. In case of SNSPD, the detector may be outside the Receiver's unit. It shall	Test Case No. 3

	have provision for a signal detection system, random number generator (may or may not depend on the protocol) and control electronics system.	
1.5	Technical Requirements of P2P QKD System	
1.5.1	A QKD source shall emit light pulses upon which quantum information is encoded. A source suitable for QKD should possess a property such that the encoded quantum information can be recovered faithfully through quantum measurement only when the measurement and encoding basis are compatible.	Type of Signal Source and Modulation characteristics covered in Test Case No. 2
1.5.2	A QKD source should be specified by the source intensity (μ), defined as the average number of photons per pulse. A QKD source should be further specified by its photon number probability distribution, p(n), defined as the probability distribution of having n photons per signal pulse.	Test Case No. 4
1.5.3	QKD system shall have provision for changing the mean photon number value. Mean photon number (with or without decoy) used in the system shall be supported by theoretic proof.	Test Case No. 5
1.5.4	QKD systems require multiple single-photon detectors for qubit detection. These detectors should be suitable for use in fibre-optic based QKD systems and shall be able to work either in gated or free running mode. Single Photon Detector (SPD) may be either of the types; i. Superconducting Nanowire Single-Photon Detector (SNSPD) or ii. Single Photon Avalanche Photo Detector (SPAD). SPD shall have a low dark count rate, low after pulse rate and low jitter. The dead time shall be of the order of ns to μs depending on the nature of the detector. QKD system shall have against known experimentally demonstrable quantum/classical channel attacks as provided in Test Guide.	Test Case No. 6 & 7
1.5.5	QKD system shall have provision for changing disclose rate.	Test Case No. 8
1.5.6	QKD system shall have provision for changing privacy amplification rate.	Test Case No. 9
1.5.7	QKD system may optionally have provision for changing information reconciliation algorithm.	Test Case No. 10
1.5.8	QKD system shall have provision for changing code rate for Information reconciliation algorithm, if applicable subjected to secured key remaining tamper proof.	Test Case No. 10
1.5.9	The system may be designed for all network topologies i.e., point-to-point or Multipoint QKD systems. QKD system for TEC Certification may be offered for Point-to-point topology without Relay nodes or P2P QKD system with relay nodes or Multipoint QKD System.	This is for information purpose.

1.5.10	QKD System shall provide the provision for Discrete Variable (DV) Quantum Key distribution protocol/distributed phase reference protocols i.e., Coherent One Way (COW), Differential Phase Shift (DPS), etc.	Record the type of QKD protocol used in the system offered for certification
1.5.11	The system shall provide at least one local and remote management interface at each node. The node shall provide a management port for Work Station connectivity with a standard connector.	Test Case No. 11
1.5.12	The connectors shall be Subscriber Connector (SC)/ Lucent Connector (LC)/ Ferrule Connector (FC)/ Straight Tip (ST) type with automatic shutters having spring action or provision of closing them manually. When out-of-use, they shall remain closed otherwise, the optical connectors shall be so positioned as be leaning towards the ground to avoid direct laser beam incidence on the user. The return loss of the optical connectors shall be ≥50dB.	Test Case No. 12
1.5.13	The Quantum Random Number Generator (QRNG) / True Random Number Generator (TRNG) may be used individually or as a seed to a Pseudo Random Number Generator (PRNG)/ Deterministic Random Bit Generator (DRBG)/NIST recommended Randomness Expansion Algorithms. The random number generator used in the system shall either be a QRNG or TRNG having a National Institute of Standards and Technology (NIST) test suite (SP800-22/90 series depending on the type of the interface and SP800-22 Diehard test, etc.) compliance as applicable.	Test Case No. 13
1.5.14	The fibre-media as stipulated in this document shall be compliant with ITUT G.652D and ITU-T G.655 NZ-DSF and ITU-T G.657 recommendations on single mode optical fibre.	Undertaking to be submitted by the manufacturer.
1.5.15	The software/hardware in the equipment shall not pose any problem due to changes in date and time caused by events such as changeover of millennium/century, leap year etc. in the normal functioning of the equipment.	Test Case No. 14
1.5.16	QKD Modules authentication shall be done by a classical channel existing between QKD Modules.	Test Case No. 15
1.5.17	QKD Module's classical channel(s), used for key post-processing, synchronization, and authentication, shall be secured using classical / Post Quantum Cryptographic (PQC) algorithms as per the requirements of the purchaser.	Test Case No. 16
1.5.18	The QKD Modules shall implement all necessary functions for supporting QKD Protocols. Such functions may include random number generation, quantum communication, distillation for key generation, quantum channel synchronization, etc.	Covered in Test Case No. 1 – 3.

1.5.19	Secret Key shall be generated by each QKD module, Both QKD modules shall be capable of delivering a key pair to the corresponding pair of the Key Managers using a standard interface as defined in ETSI GS QKD 014. Further, the equipment may also support other interfaces e.g. Secure Key Integration Protocol (SKIP), etc. as per the requirements of the purchaser.	Test Case No. 17
1.5.20	The QKD module shall provide status information for the module and the associated QKD link through a secure management interface.	Covered in Test case No. 11
1.5.21	The QKD module shall extend a sign out or alarm signal to the user as and when the QBER threshold is exceeded to indicate the possible presence of an eavesdropper for necessary corrective action.	Test case No. 18
1.5.22	The Key Manager shall provide elements of key life cycle management key ID, QKD module ID, key generation date, name of the cryptographic application to which the key is supplied, key supply date, etc.	Test Case No. 19
1.5.23	The Key Manager shall apply the key management policy. Key management policy may include deleting the keys or preserving the keys in key storage after the key supply has been executed.	Test Case No. 20
1.5.24	Once Keys are provided by Key Manager to the user network: i. The Key Manager shall receive key requests from authorized cryptographic applications through the key supply interface. ii. The Key Manager shall supply the requested number of keys to a cryptographic application in the service layer of the user network through the key supply interface. iii. The Key Manager shall supply keys to cryptographic applications in the service layer of the user network through the key supply interface with security capabilities.	Test Case No. 21
1.5.25	The Quantum Key Distribution Transmitter and Quantum Key Distribution Receiver shall support tamper-evident enclosure and secure tamper-event logging.	Test Case No. 22
1.6	**Technical Requirements for Star Topology**	
1.6.1	The Bob node shall function as the central coordinating node, with multiple Alice nodes connected in a star topology	Test Case No. 23
1.6.2	The Hub shall include an optical switch as a stand-alone unit or integrated into QKD module to support optical switching.	Physically check and note down the observations.
1.6.3	The system shall support automatic optical switching between different connected Alice nodes without any manual intervention.	Test Case No. 23
1.6.4	The switching time between connected nodes shall be user-configurable.	Test Case No. 23

1.6.5	The system shall support the connection of atleast 2 Alice nodes to the central coordinating node.	Test Case No. 23
1.6.6	The Hub (Bob) shall act as key relay to establish a secure connection using QKD keys between Alice nodes.	Test Case No. 23
1.6.7	All the nodes shall provide QKD secure Keys to the cryptographic applications using standard ETSI GS QKD 014.	Repeat Test Case No. 17 for all QKD nodes in the topology.
1.7	Performance Requirement of QKD System	
1.7.1	Online Performance Monitoring The QKD modules shall provide performance information of the QKD module. The online monitoring of the QKD system shall provide the facility for locally and remotely monitoring of some important parameters. The system shall monitor and report optical layer performance in real time to Local Craft Terminal (LCT)/ Element Management System (EMS). The system shall have provision to monitor the following parameters: i. Quantum Bit Error Rate (QBER) ii. Key Rate iii. Visibility (applicable for COW protocol) iv. Mean Photon Number v. SPD parameters like dead time, efficiency, etc. vi. Quantum channel transmit power vii. On-demand randomness testing viii. Key symmetry	Test Case No. 24
1.7.2	QBER performance shall be less than 5% (desirable) for the Quantum Channel Loss specified in table 1. QBER may increase and key rate may decrease for higher Quantum Channel loss. The same may be specified by the procurer, based on their requirements.	Covered in Test Case No. 18
1.7.3	Visibility performance (for COW QKD) over a simulated section shall be tested for 24 hours and visibility performance shall be better than 90%.	For COW protocol, verify that the visibility performance is better than 90% over 24 hours. Record the observations.
1.8	Technical Specifications of QKD System	

<table>
<tr><td>1.8.1</td><td>Window of operation – The optical window of operation of the Quantum shall be in the range from 1530nm to 1565 (C-band) as per ITU-T Rec. G.694.1.</td><td>Covered in Test Case No. 2</td></tr>
<tr><td>1.8.2</td><td>Communication protocol and data format for a quantum key distribution (QKD) network to supply cryptographic keys to an application entity (router/switch, etc.) shall be as per the ETSI standard.
Table 1: Specifications
<table>
<tr><th>S.No.</th><th>Specification Description</th><th colspan="4">Value</th></tr>
<tr><td rowspan="2">1.</td><td rowspan="2">Secure Key Rate</td><td colspan="4">>2Kbps for DPS protocol at the maximum channel loss declared by the manufacturer</td></tr>
<tr><td colspan="4">>1Kbps for COW protocol at the maximum channel loss declared by the manufacturer</td></tr>
<tr><td>2.</td><td>QBER</td><td colspan="4"><5%</td></tr>
<tr><td>3.</td><td>Key transfer Interface</td><td colspan="4">UART/USB/Ethernet</td></tr>
<tr><td>4.</td><td>Quantum Wavelength</td><td colspan="4">C-Band @ITU-T DWDM grid</td></tr>
<tr><td>5.</td><td>Optical Return Loss</td><td colspan="4">>50dB</td></tr>
<tr><td>6.</td><td>Mean Photon Number</td><td colspan="4">Default value:
Range:</td></tr>
<tr><td>7.</td><td>Disclose Rate</td><td colspan="4">Default value:
Range:</td></tr>
<tr><td>8.</td><td>Privacy Amplification Rate</td><td colspan="4">Default value:
Range:</td></tr>
<tr><td>9.</td><td>Information Reconciliation Algorithm</td><td colspan="4"></td></tr>
<tr><td>10.</td><td>Fibre Type</td><td colspan="4">G.652D, G.655, G.657</td></tr>
<tr><td>11.</td><td>Quantum Channel Loss for distributed phase reference</td><td>Type of the product application</td><td>Short Range</td><td>Long Range</td><td>Extended Range</td></tr>
</table></td><td>Test Case No. 25</td></tr>
</table>

			protocols	Channel Loss typical	Upto 12dB	Upto 18dB	Greater than 18 dB
	12.	Operating Temperature	10 to 25 °C				
	13.	Detector Type	SPD (SPAD / SNSPD /etc.)				
	14.	Power Supply	230V AC@50Hz or -48 V DC				
	15.	Mechanical Dimension of the rack	Width- 483 mm (19") Height- n*1U (1U ~ 45 mm) Depth - ≤ 800 mm Access - Front/back (Pizza box solution shall be mountable in a rack with the above dimensions)				
	16.	Synchronization	Over Classical Channel				
1.9	Technical Requirements of Multipoint QKD System						
1.9.1	Multipoint QKD System shall have the following additional technical requirements in addition to technical requirements mentioned in Clauses 2.3, 2.4 and 2.5 for P2P QKD System.						This is for information purpose.
1.9.2	A Multipoint QKD system shall include: i. **Key Manager:** To receive and manage keys generated by QKD modules and QKD links, relay the keys, and supply the keys to cryptographic applications. Key Manager functionality may be applicable for P2P QKD systems also. ii. **QKDN Controller:** To control QKDN resources to ensure secure, stable, efficient, and robust operations of a QKDN. iii. **QKDN Manager:** To manage fault, configuration, accounting, performance and security (FCAPS) aspects of a QKDN as a whole, and support user network management.						This is for information purpose.
1.10	Technical Requirements of Key Manager: The Key Manager shall receive keys from a QKD module(s) via an appropriate interface, and store them securely.						Covered in signalling procedures specified in 1.14.

1.10.1	The Key Manager may perform the following tasks: Key re-size, key reformat (necessary headers and footers such as key ID, generation date, key length, etc., for key management), key storage. The Key Manager shall format keys where necessary for internal purposes or for key supply or key relay, including combining or splitting where lengths are not appropriate.	Test Case No. 26
1.10.2	The Key Manager shall be compatible with various kinds of QKD modules which implement different protocols. The manufacturer may provide the details of QKD protocols supported by the Key manager.	Details to be submitted by the manufacturer.
1.10.3	The Key Manager shall receive status information of QKD module(s) and QKD link(s) from the QKD module(s) in the quantum layer. In implementations employing SDN-based control of QKD networks, the status information may be logged in the network control layer instead of the key manager.	Test Case No. 27
1.10.4	The Key Manager (KM) shall provide information on key management for QKDN control/management functions to the QKDN controller. Such information on key management may include information such as which QKD module the key comes from, which node the key is relayed to, timestamp, the cryptographic application to which the key is supplied, shared key amount of a KM link, key consumption rate, KM link status, accounting and alarm on fault.	Test Case No. 27
1.10.5	The Key Manager shall provide fault and performance information of the Key Manager and Key Manager links to the QKDN manager.	Test Case No. 27
1.10.6	The Key Management unit shall include secure hardware to store the generated keys. Appropriate key manager units are essential for the effective last-mile delivery of quantum keys to the end-user applications. The secure hardware implementation may be done through HSM or TPM etc. which may be decided by the procurer and mentioned during offering the product for testing.	Test Case No. 28
1.10.7	The Key Manager shall support key relay employing highly secure encryption (eg; one-time pad (OTP)) via trusted node(s) to establish keys between any two remote KMs connected to a QKDN with three or more nodes. In case the necessary number of keys for an IT-secure key relay is not available, keys may be relayed by another appropriate method according to key management policy (such as AES).	Already covered in Test Case No. 27 Clause 1.18 - Signalling procedures for Key Relay
1.10.8	The Key Manager may have capabilities of key synchronization, entity authentication and message authentication to make Key Relaying reliable and secure.	Test Case No. 27
1.10.9	The Key Managers may cooperate with each other under the control of the QKDN controller to make key relay efficient.	Already covered in Clause 1.18 - Signalling

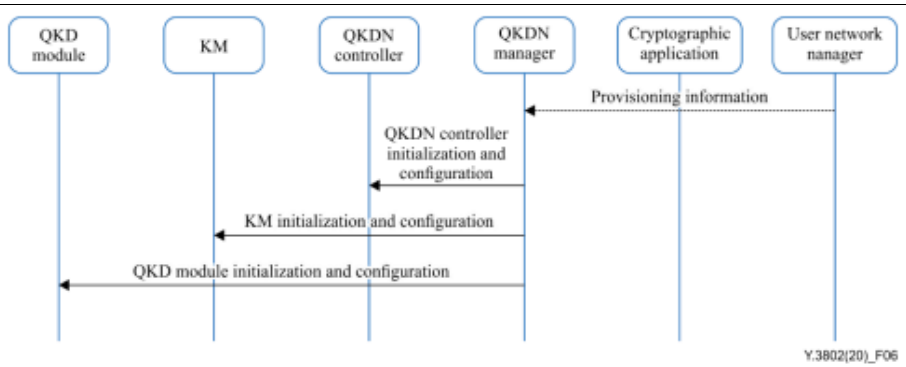
		procedures for Key Relay
1.10.10	The Key Manager may present a key supply interface that various cryptographic applications in the service layer of the user network can utilize. Cryptographic applications may have diverse requirements and run-on various environments. The Key Manager may support access control of cryptographic applications.	Already covered in Test Case No. 17, 19, 20, 21 and Operational procedures for Key supply in clause 1.15 and 1.16.
1.10.11	The Key Manager shall present a key supply interface that various cryptographic applications can utilize to send key requests.	
1.10.12	The Key Manager shall supply the requested number of keys to a cryptographic application in the service layer of the user network via a key supply interface, subject to any key management policies, when sufficient keys are available.	
1.10.13	The Key Manager shall supply keys to cryptographic applications via a key supply interface with security capabilities.	
1.10.14	The Key Manager shall support access control of cryptographic applications.	
1.10.15	The Key Manager shall provide elements of key life cycle management (key ID, QKD module ID, key generation date, name of cryptographic application to which the key is supplied, key supply date, etc.).	
1.11	Technical Requirements of QKDN Controller:	
1.11.1	The QKDN controller shall control key relay routes including rerouting between the two endpoints of cryptographic applications which require the key.	Test Case No. 29
1.11.2	The QKDN controller shall control the status of the key management layer and quantum layer.	QKDN controller shall control the status of the quantum layer and the key management layer by executing functions like session control, configuration, and routing. Already covered in Operational procedures of QKDN.
1.11.3	The QKDN controller shall control the reconfiguration of the QKD link if failure or eavesdropping occurs.	Test Case No. 29

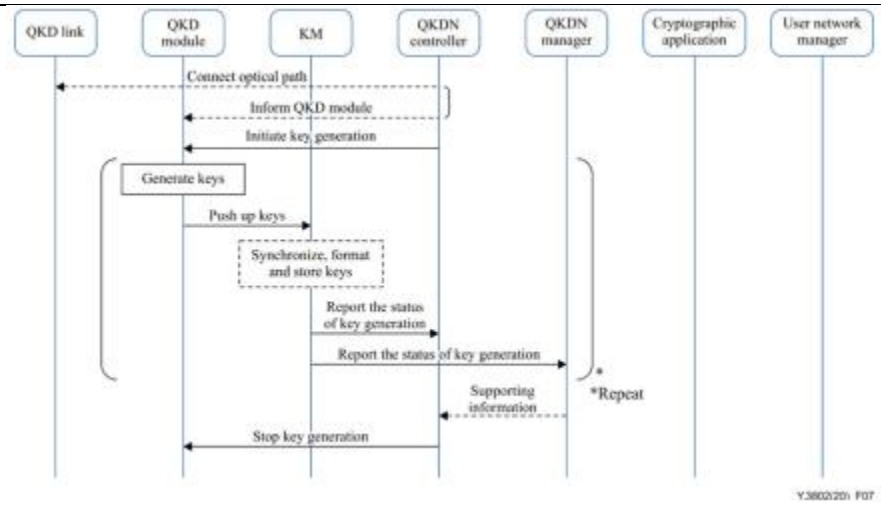
1.11.4	The QKDN controller shall provide fault, performance, accounting, and configuration information to a QKDN manager.	Test Case No. 29
1.11.5	The QKDN controller shall perform the following tasks: control of Key Managers and Key Manager links, control of QKD modules and QKD links, authentication and authorization control, etc.	Test Case No. 29
1.11.6	The QKDN controller may provide charging policy control.	Test Case No. 29
1.11.7	The QKDN controller may provide session control. The session is the communication between KMs to establish the end-to-end key or to supply keys to cryptographic applications in the service layer of the user network. The session control initiates, maintains, and terminates the session.	Already covered in Operational procedures of QKDN
1.11.8	The QKDN controller may provide quality of service (QoS) policy control.	Test Case No. 29
1.11.9	The QKDN controller may support and ensure access control of functional elements in the quantum layer and the key management layer.	Test Case No. 29
1.12	Technical Requirements of QKDN Manager:	
1.12.1	The QKDN manager shall support fault management, accounting management, configuration management, performance management and security management.	Test Case No. 30
1.12.2	The QKDN manager shall provide fault management to support: i. collecting/receiving status information provided by the quantum, key management, and QKDN control layers; ii. analysing the status information collected/received for fault indicators.	Test Case No. 30
1.12.3	The QKDN manager is required to provision and configure the managed resources in each layer.	Test Case No. 30
1.12.4	The QKDN manager is required to support routing and rerouting of key relay.	Covered in operational procedures of QKDN
1.12.5	The QKDN manager may support management of the network topology.	Test Case No. 30
1.12.6	The QKDN manager may perform inventory management for all the QKDN resources in each layer.	Test Case No. 30
1.12.7	The QKDN manager may manage the life cycle of the resource repositories (e.g., create, store, retrieve, modify, remove, etc.) in each layer.	Test Case No. 30
1.12.8	The QKDN manager shall monitor QKD link failures to support QKD modules for appropriate recovery actions including reconfiguration of QKD links and rerouting of key relay routes.	Test Case No. 30

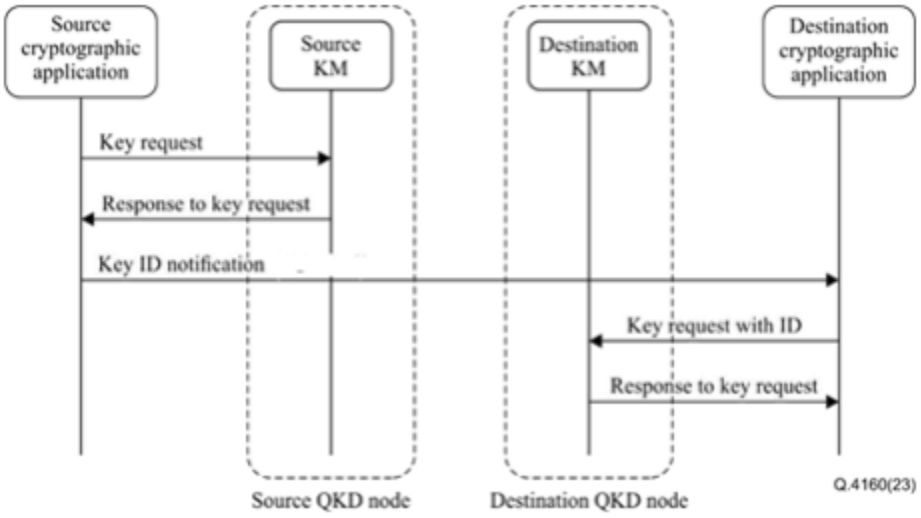
1.12.9	The QKDN manager may provide fault detection and root-cause analysis/diagnosis capability for quantum, key management, and QKDN control layers.	Test Case No. 30
1.12.10	The QKDN manager may make decisions and generation failure resolving policies and interacts with each layer for correction of faults.	Test Case No. 30
1.12.11	The QKDN manager may discover each layer managed resources and functions and bootstrap to make them ready for the operation based on the bootstrapping policies. The QKDN manager is recommended to measure the resource usage data of each layer (e.g., usage of quantum keys in a quantum layer) and generates accounting policies for charging.	Test Case No. 30
1.12.12	The QKDN manager shall collect the performance data and status of each layer, register them into a performance database and updates them.	Test Case No. 30
1.12.13	The QKDN manager shall analyse the performance of collected data and generate performance reports (Performance Management).	Test Case No. 30
1.12.14	The QKDN manager shall manage the key supply service policies (Performance Management).	Test Case No. 30
1.12.15	The QKDN manager shall collect management information including event logs, audit trails, and so on from each layer for detecting security anomalies.	Test Case No. 30
1.12.16	The QKDN manager shall support key life cycle management by KMs, ensuring traceability of keys by using the log database.	Already covered in Test Case No. 19
1.12.17	The QKDN manager may have a root certification authority which issues root certificates to the QKDN controller. The QKDN manager shall support the QKDN controller for the access control.	Test Case No. 30
1.12.18	The QKDN manager may manage the key management policies and transmits them to the QKDN controller.	Test Case No. 30
1.12.19	The QKDN manager may perform cross-layer management orchestration and also to support management requests from a user network management.	Test Case No. 30
1.12.20	The QKDN manager shall monitor the status of the whole QKDN.	Test Case No. 30
1.12.21	The QKDN manager shall authenticate and authorize management. For example, management of the identification and registration of modules in a QKDN, and their access rights.	Test Case No. 30
1.12.22	The QKDN manager may provide QoS management and charging management.	Test Case No. 30
1.12.23	The QKDN manager shall detect eavesdropping attempts against a quantum channel.	Test Case No. 30

1.12.24	The QKDN manager may optionally provide availability and reliability of quantum key distribution based on the redundancy of QKD links provided by the quantum layer.	Test Case No. 30
1.12.25	The QKDN manager shall support the QKDN controller for routing and rerouting of key relays including instruction of policies and rules caused by the faults or performance degradation.	Test Case No. 30
1.12.26	The QKDN manager may optionally provide the QKDN resource provisioning requested by the user network manager.	Test Case No. 30
1.12.27	The QKDN manager may optionally provide management orchestration of the QKDN control layer and QKDN management layer to support the QKDN controller to take necessary actions for anomalous situations (e.g., fault, performance degradation, security attacks, etc.).	Test Case No. 30
1.12.28	QKDN manager shall provide a graphical user interface (GUI) for network monitoring and management.	Test Case No. 30
1.12.29	QKDN manager shall support Multi-Factor Authentication (MFA) for all administrative and privileged user access.	Test Case No. 30
1.12.30	QKDN manager shall provide a secure, auditable interface for defining new roles in addition to predefined roles. All changes to roles and their permissions shall be logged with a timestamp and the user ID of the administrator making the change.	Test Case No. 30
1.12.31	QKDN Manager shall support the definition and enforcement of granular key delivery policies that govern the provisioning of cryptographic keys to user applications and services based on a predefined set of criteria like QKD peers, app expiry, TTL, interface type.	Test Case No. 30
1.12.32	QKDN manager shall support the orchestration and management of multiple QKDN controllers. This capability is essential for managing large-scale, heterogeneous, and multi-domain QKD networks, enabling a unified view and centralized control.	Test Case No. 30
1.12.33	The QKDN shall adopt common data models for telemetry (e.g., YANG models or JSON schemas) to describe quantum-layer metrics (QBER, photon count, key rate), KM metrics (secure-key balance, consumption rate), and control-layer status to ease integration.	Test Case No. 31
1.12.34	The QKDN shall record all configuration changes, policy updates, and operator actions in an auditable change-history store.	Already covered in clause 1.12.30
1.12.35	The QKDN shall have network control and management capabilities.	Already covered in clause 1.11 and 1.12

1.12.36	The QKDN shall have the capability to contain an interface between the user network and the QKDN to supply keys in an appropriate key format to various applications.	Covered in Test Case No. 17
1.12.37	The QKDN shall have the capability to use optical fibre channels or direct free space optical channels for quantum channel networking.	The declaration in this regard to be submitted by the manufacturer.
1.12.38	The QKDN shall be capable of automatically authenticating and operating QKD nodes that are rebooted.	Test Case No. 32
1.12.39	The QKDN may have the capability to manage QoS by taking into account the request from the user network.	Already covered in clause 1.11.8 and 1.12.22
1.12.40	The QKDN shall have a unique identifier for QKD link and the same shall be provided to the QKD controller for key routing. For the key relay, modules in each node have to be identified.	Test Case No. 33
1.12.41	The communication interface between the QKD Module, QKDN controller and the QKDN manager shall be secured, using Classical or Post Quantum Cryptographic Algorithms.	Test Case No. 34
1.12.42	QKDN manager and QKDN controller may optionally support a High Availability (HA) deployment. This architecture shall ensure continuous operation of the QKDN manager and QKDN controller. This can be achieved through either of these options: i. **Active-Standby:** An active primary instance is backed up by a redundant standby instance, ready to take over in case of a failure. ii. **Active-Active:** Multiple instances run simultaneously, sharing the workload and providing instant failover.	Test Case No. 35
1.12.43	The equipment may support Dual stack IP addresses (IPv4 & IPv6) for management and services.	Test Case No. 36
1.13	**Operational Procedures for the QKDN:**	
1.13.1	Service provisioning and system initialization procedure The below figure illustrates a procedure for service provisioning and system initialization for a multi-point QKD system.	Test Case No. 37

	 *Figure 6 Service provisioning and system initialization procedure* The signalling procedures shall be as defined as per the ITU-T / ETSI standards. There are two alternatives for service provisioning. i. In case where a user network manager is in charge of service provisioning, the user network manager provides service provisioning information including profiles of cryptographic applications to a QKDN manager. ii. On the other hand, in case where the QKDN manager is in charge of service provisioning as standalone mode, the QKDN manager uses its own service provisioning information directly. According to the provisioning information, the QKDN manager initiates the action of a QKDN controller, a KM and a QKD module to initialize and configure a QKDN. The sequence of the initialization and configuration of the QKDN controller, the KM and the QKD module can be in arbitrary order.	
1.14	Key generation procedure The below figure illustrates a procedure for key generation in multi-point QKD system.	Test Case No. 38

	 *Figure 7 Key generation procedure* i. A QKDN controller optionally instructs to initiate the connection of an optical path in a QKD link and informs QKD modules of the initiation result if necessary. ii. The QKDN controller may optionally send request to QKDN modules to initiate key generation. The key generation may also automatically start between QKD modules after system initialization. iii. The QKD modules send and/or receive quantum signals and then perform synchronization of quantum signals and key distillation for key generation. iv. The QKD modules push up the generated keys to KMs. v. The KMs optionally synchronize, format and store these keys if necessary. vi. The KMs report the status of key generation to the QKDN controller and the QKDN manager for control and management functions respectively. vii. The sequence from step 3 to step 6 can be repeated (and often executed in parallel) until a sufficient number of keys are generated. viii. The QKDN manager optionally sends supporting information to the QKDN controller if necessary. ix. The QKDN controller may optionally request to stop key generation to the QKD modules due to the completion of key generation or other reasons, if required.	
1.15	Key supply upon request mode: The below figure shows typical signalling procedures for key supply upon request mode implemented by two QKD nodes in a multipoint QKDN system	Test Case No. 39

	 *Figure 8 Signalling procedures for key supply upon request mode implemented by two QKD nodes* i. The source cryptographic application sends a "key request" message to the source KM at the source QKD node. ii. The source KM responds "response to key request" message to the source cryptographic application with the keys requested and the corresponding key IDs. iii. The source cryptographic application sends a "key ID notification" message to the destination cryptographic application with the key IDs. iv. The destination cryptographic application sends a "key request with ID" message with the received key IDs to the destination KM at the destination QKD node. v. The destination KM responds "response to key request" message to the destination cryptographic application with the keys requested.	
1.16	Proactive key supply mode: In the mode, the KM at the source QKD node initiates a key supply upon request, and then instructs the KM at the destination QKD node to make a proactive key supply. The proactive key supply mode can be adopted in scenarios where the cryptographic applications on both sides are restricted to having no direct communication before they have KSA-keys. The below figure signalling procedures for proactive key supply mode implemented by two QKD nodes.	Test Case No. 40

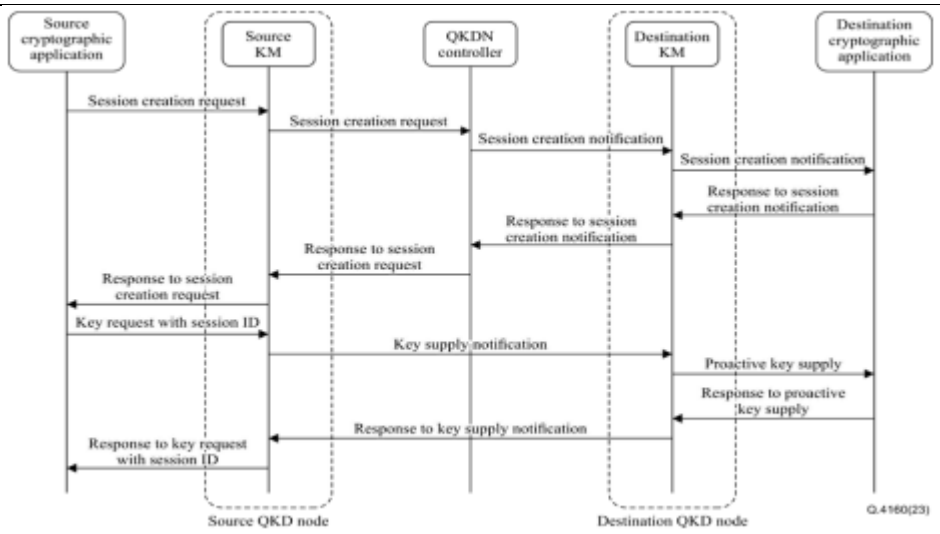


Figure 9 Typical signalling procedures for proactive key supply mode implemented by two QKD nodes

i. The source cryptographic application sends a "session creation request" message to the source KM at the source QKD node.

ii. The source KM sends a "session creation request" message to the corresponding QKDN controller.

iii. The QKDN controller generates a session ID and sends a "session creation notification" message with the session ID to the destination KM at the destination QKD node. If there are distributed QKDN controllers, the "session creation notification" message will be sent from the QKDN controller at the source QKD node to the QKDN controller at the destination QKD node, and then relayed to the destination KM.

iv. The destination KM sends a "session creation notification" message with the received session ID to the destination cryptographic application.

v. The destination cryptographic application responds "response to session creation notification" message to the destination KM with the session creation result.

vi. The destination KM responds "response to session creation notification" message to the corresponding QKDN controller with the received session creation result. If there are distributed QKDN controllers, the "response to session creation notification" message will be sent from the destination KM to the QKDN controller at the destination QKD node, and then relayed to the QKDN controller at the source QKD node.

	vii. As the session is successfully created, the QKDN controller responds "response to session creation request" message to the source KM with the session ID in the source QKD node. viii. The source KM responds "response to session creation request" message to the source cryptographic application with the received session ID. ix. The source cryptographic application sends a "key request with session ID" message to the source KM in the source QKD node with the received session ID. x. The source KM in the source QKD node sends a "key supply notification" message to the destination KM in the destination QKD node with the number of keys to be supplied. xi. The destination KM sends a "proactive key supply" message to the destination cryptographic application with the notified number of keys. xii. The destination cryptographic application responds "response to proactive key supply" message to the destination KM with the key IDs of the received keys. xiii. The destination KM responds "response to key supply notification" message to the source KM with the received key IDs. xiv. The source KM responds "response to key request with session ID" message to the source cryptographic application with keys corresponding to the received key IDs.	
1.17	Key relay for a distributed QKDN (1) The figure shows typical signalling procedures for key relay for a distributed QKDN. KM1 starts signalling procedures for the key relay to the corresponding QKDN controller. i. The KM1 in the QKD node 1 sends a "key relay request notification" message to the QKDN controller in the trusted node, and the QKDN controller responds "key relay request" message with the full key relay route to the destination node. ii. The KM1 starts the key relay according to the key relay route. The KM1 sends a "key relay" message to the KM2 in the QKD node 2. iii. The KM2 in QKD node 2 performs a key relay to the KM3 in the QKD node 3 according to the key relay route. iv. When the key reaches the destination QKD node which is the nearest node to the destination cryptographic application, the KM (shown as	Test Case No. 41

KM3 in the figure) sends "key relay completion notification" message to the source KM (shown as KM1 in the figure), then the KM1 sends "response to key relay request" message to the QKDN controller in the trusted node.

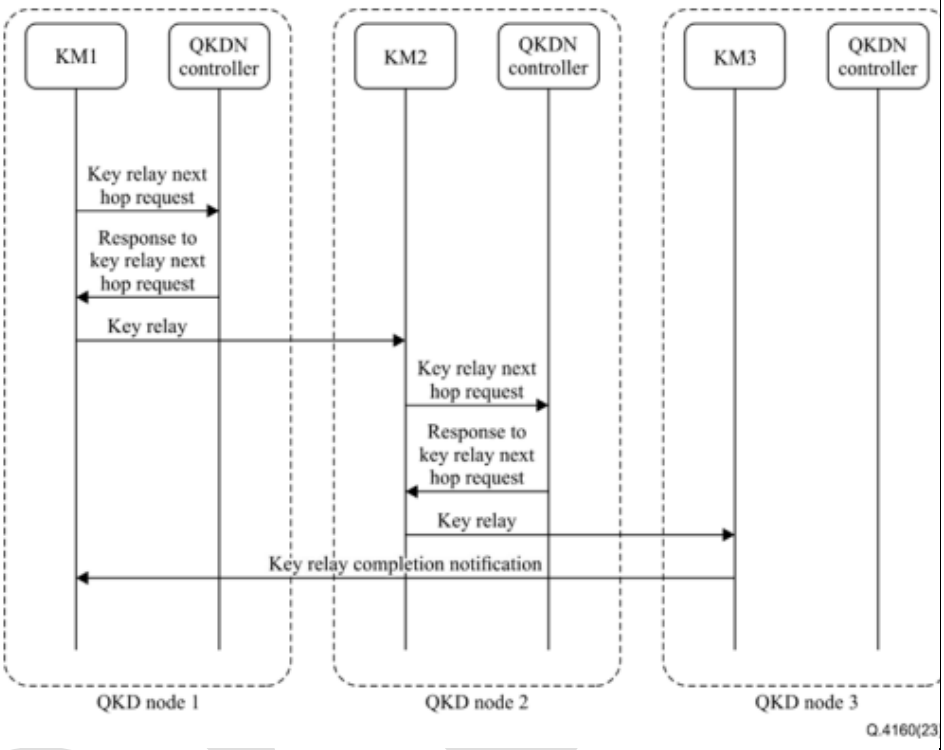


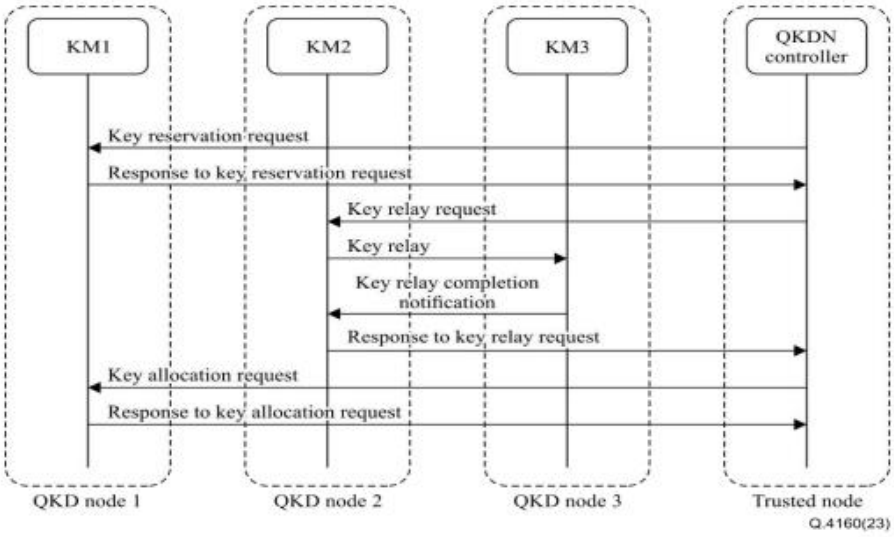
Figure 10A Typical signalling procedures for key relay for a distributed QKDN

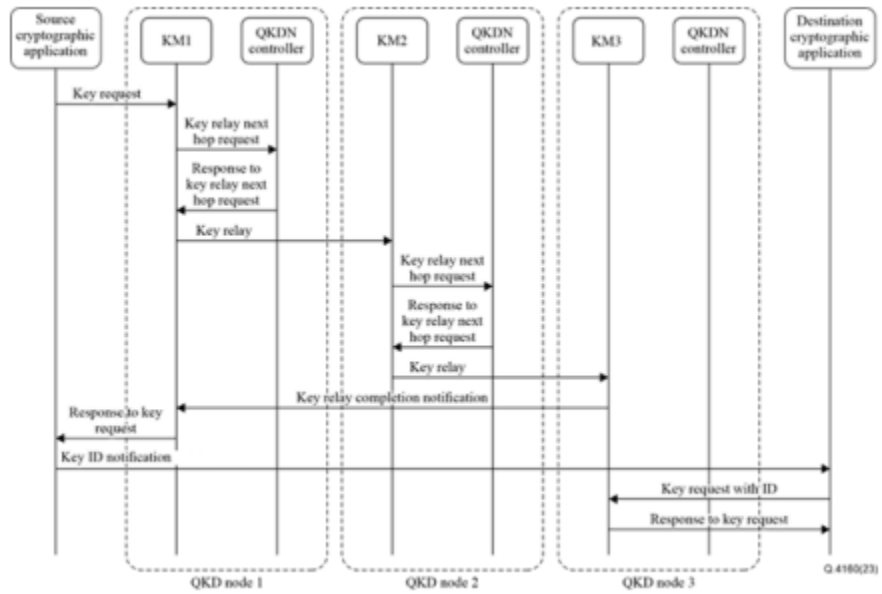
(2) The below figure shows typical signalling procedures for key relay for a centralized QKDN with key reservation:

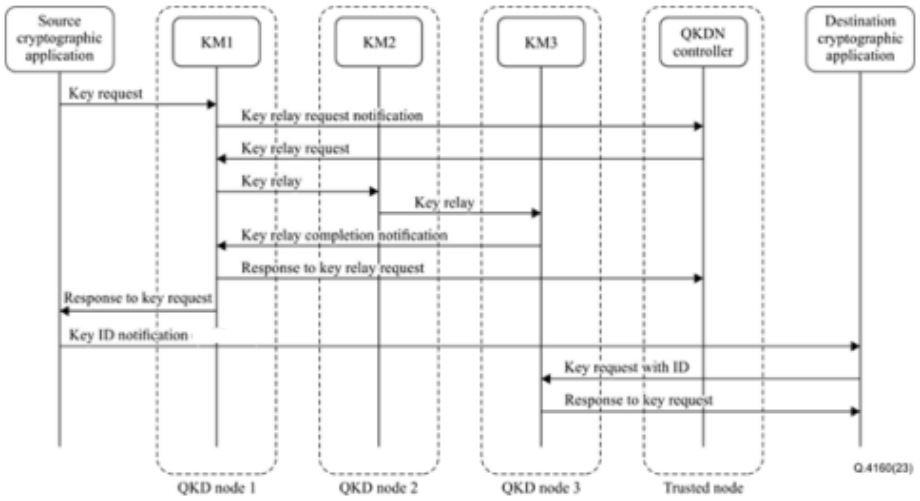
i. The QKDN controller sends a "key reservation request" to the KM1 to reserve the key that will be relayed to the destination KM. The KM1 sends a response to the QKDN controller by "response to key reservation request".

ii. Then the corresponding QKDN controller sends a "key relay request" message to the KM2 with the full key relay route to the destination node, and the KM2 starts the key relay.

iii. When the key reaches the destination QKD node which is the nearest node to the destination cryptographic application, the KM (shown as KM3 in the figure) sends "key relay completion notification" message to the source KM (shown as KM2 in the figure), then the KM2 sends

	"response to key relay request" message to the QKDN controller in the trusted node. iv. The QKDN controller sends a "key allocation request" to allocate the reserved key to share with the destination KM3, and KM1 responds to the QKDN controller with "response to key allocation request" message in the trusted node.  *Figure: 10B Typical signalling procedures for key relay for a centralized QKDN with key reservation*	
1.18	Key request, key relay, and key supply	
1.18.1	Distributed QKDN: The below figure shows typical signalling procedures for key request, key relay, and key supply for a distributed QKDN: i. The source cryptographic application sends a "key request" message to the KM1 in the QKD node 1, which is the nearest node of the source cryptographic application. ii. The KM1 sends "key relay next hop request" message to the QKDN controller in the QKD node 1, and the QKDN controller responds "response to key relay next hop request" message with the next hop destination for key relay, then the KM1 relays the key along with the response to the KM2.	Test Case No. 42

	 *Figure: 11A Typical signalling procedures for key request, key relay, and key supply for distributed QKDNs* iii. The KM2 and the QKDN controller in the QKD node 2 performs the same procedures as the KM1 of the QKD node 1. iv. When the key reaches the destination QKD node which is the nearest node to the destination cryptographic application, the KM (shown as KM3 in the figure) sends "key relay completion notification" message to the source KM (shown as the KM1 in the figure), then the KM1 responds "response to key request" message to the source cryptographic application with keys. v. The source cryptographic application sends a "key ID notification" message to the destination cryptographic application with a key ID. vi. The destination cryptographic application sends a "key request with ID" message with key ID which was received from the source cryptographic application (see step 5) to the nearest KM (shown as KM3 in the figure). vii. The nearest KM (shown as KM3 in the figure) responds "response to key request" message with keys to the destination cryptographic application.	
1.18.2	Centralized QKDN: The figure shows typical signalling procedures for key request, key relay, and key supply for a centralized QKDN. i. The source cryptographic application sends "key request" message to the KM1 in the QKD node 1, which is the nearest node of the source cryptographic application.	Test Case No. 42

	ii. The KM1 sends "key relay request notification" message to the QKDN controller in the trusted node, and the QKDN controller responds "key relay request" message with the full key relay route to the destination node.  Figure: 11B – Typical signalling procedures for key request, key relay, and key supply for centralized QKDNs iii. The KM1 starts key relay along with the key relay route. The KM2 in QKD node 2 performs key relay according to the key relay route. iv. When the key reaches the destination QKD node which is the nearest node to the destination cryptographic application, the KM (shown as KM3 in the figure) sends "key relay completion notification" message to the source KM (shown as KM1 in the figure), then the KM1 sends "response to key relay request" message to the QKDN controller in the trusted node, and also responds "response to key request" message to the source cryptographic application with keys. v. The source cryptographic application sends "key ID notification" message to the destination cryptographic application with the key ID. vi. The destination cryptographic application sends "key request with ID" message with a key ID which was received from the source cryptographic application (see step 5) to the nearest KM (shown as KM3 in the figure). vii. The nearest KM (shown as KM3 in the figure) responds "response to key request" message with keys to the destination cryptographic application.	
	CHAPTER 2	
	General Requirements	
2.1	Reference documents	

2.1.1	Whatever that has not been specifically stated in this document, shall be deemed to be as per relevant latest ITU-T Recommendations.	This is for information purpose.
2.1.2	Relevant ITU-T Recommendations & other specifications are given in the GR.	This is for information purpose.
2.1.3	All references to TEC GRs & other Recommendations imply their latest issues.	Declaration shall be submitted.
2.2	Engineering requirements	
2.2.1	The manufacturers shall furnish the actual dimensions and weight of the equipment.	Record the dimensions and weight of the equipment.
2.2.2	The equipment shall be housed in an ETSI standard 19" rack up to 800 mm depth with front/back access or as per ETSI standard.	Physically inspect and record the observations.
2.2.3	The system shall work in an environment with 10°C to 25°C temperature and 80% Rh.	Covered in Environment Testing.
2.2.4	It should be engineered to comply with environmental test requirements as defined in this document.	
2.2.5	The external plug-in units shall be of a suitable type to allow their removal/insertion while the equipment is in energized condition.	Physically inspect and record the observations.
2.2.6	The mechanical design and construction of each card/unit shall be inherently robust and rigid under all conditions of operation, adjustment, replacement, storage and transport.	Physically inspect and record the observations.
2.2.7	Each sub-assembly shall be marked with schematic reference to show its function so that it is identifiable from the layout diagram in the handbook	Physically inspect and record the observations.
2.2.8	Each terminal block and individual tags shall be numbered suitably with a clear identification code and shall correspond to the associated wiring drawings.	Physically inspect and record the observations.
2.2.9	All external Interfaces / Controls / Indicators/Switches shall be clearly screen printed/marked on the unit to show their functional/connectivity diagrams and functions.	Physically inspect and record the observations.

2.2.10	Important Do's and Don'ts about the operation of the system shall be indicated.	Physically inspect and record the observations.
2.3	Operational requirements	
2.3.1	The equipment shall be designed for continuous operation.	Covered in Clause 2.12
2.3.2	The equipment shall be able to perform satisfactorily without any degradation at an altitude up to 4000 meters above mean sea level. A test certificate from the manufacturer will be acceptable, in case no test facility is available.	Test certificate from the manufacturer shall be submitted or Testing shall be carried out at an altitude up to 4000 meters above mean sea level to check whether the system works satisfactorily.
2.3.3	Visual indication to show power ON/OFF status shall be provided.	Physically inspect and record the observations.
2.3.4	Wherever the visual indications are provided, green colour for healthy and red colour for unhealthy conditions would be provided. Some colours may be used for non-urgent alarms.	Physically inspect and record the observations.
2.4	Quality requirements	
2.4.1	The manufacturer shall furnish the MTBF value along with the methodology used for calculation. The minimum value of MTBF shall be 25,000 hrs.	The values shall be submitted by the manufacturer along with the calculation methodology.
2.4.2	The equipment shall be manufactured in accordance with the international quality management system ISO 9001:2015 or latest issue. A quality plan describing the quality assurance system followed by the manufacturer would be required to be submitted by the manufacturer.	Declaration/Certificate to be submitted for ISO 9001:2015 compliance.

		The Quality plan describing the quality assurance system shall be submitted by the manufacturer along with the quality check report of the finished product.
2.5	Maintenance requirements	
2.5.1	Maintenance philosophy is to replace faulty units/subsystems after quick online analysis through monitoring sockets, alarm indications and Built-in Test Equipment	The details shall be provided by the manufacturer.
2.5.2	The equipment shall have easy access for servicing and maintenance.	Physically inspect and record the observations.
2.5.3	Suitable alarms shall be provided for the identification of faults in the system and faulty units.	Test Case No. 43
2.5.4	Ratings and types of fuses used are to be indicated by the supplier.	Physically inspect and record the observations.
2.6	Power supply requirements for QKD Equipment	
2.6.1	The QKD system may be provided with two power feeds. i. centralized power supply with 1+1 redundancy and ii. Distributed onboard power supply.	Inspect and Record the Power supply details of the system including Make and Ratings: voltage, current, frequency (if applicable).
2.6.2	The equipment should work at a single phase AC mains supply of 230 V with variation in the range of +10% and -15% and frequency as 50 Hz +/-2Hz or uninterrupted –48V DC with a variation in the range from -40V to -60V.	Test Case No. 44

2.6.3	The equipment shall operate over this range without any degradation in performance.	Test Case No. 44
2.6.4	The equipment shall be adequately protected in case of voltage variation beyond the range mentioned above and also against input reverse polarity in case of DC feeds.	Test Case No. 44
2.6.5	The derived DC voltages in the equipment shall have protection against over-voltage, short-circuit and overload.	Test Case No. 44
2.6.6	The equipment shall be power efficient. The actual power rating/ consumption is to be furnished by the manufacturer of the equipment.	The power consumed by the equipment in idle state and in the operating state shall be noted.
2.7	Accessories	
2.7.1	The supplier shall provide a complete set of: i. All the necessary connectors, connecting cables and accessories are required for satisfactory and convenient operation of the equipment. Types of connectors, adapters to be used and accessories of the approved quality shall be indicated in the operating manuals which should conform with the detailed list in the GR. ii. Software, along with software version and the arrangement to load the software at site.	The details shall be provided by the manufacturer.
2.8	Documentation Technical literature in English with complete layout, detailed block schematic and circuit diagram of various assemblies with test voltages/ waveforms at different test points of the units shall be provided in hard copy. Additionally, a soft copy /QR code on the system in respect of technical literature may be provided both in Hindi and English. All aspects of installation operation, maintenance and repair shall be covered in the manuals.	The details shall be provided by the manufacturer.
2.8.1	Installation, operation and maintenance manual It should cover the following: i. Safety measures to be observed in handling the equipment; ii. Precautions for installation, operation and maintenance; iii. Test jigs and fixtures required and procedures for routine maintenance, preventive maintenance, troubleshooting and sub-assembly replacement; iv. Illustration of internal and external mechanical parts.	Check whether the Installation, operation and maintenance manual provided by the manufacturer

		covers the required aspects.
2.8.2	Repair Manual It should cover the following: i. List of replaceable parts used to include their sources and the approving authority ii. Detailed ordering information for all the replaceable parts shall be listed in the manual to facilitate the reordering of spares. iii. Procedure for trouble-shooting and sub-assembly replacement shall be provided. Test fixtures and accessories required for repair shall also be indicated. A systematic troubleshooting chart (fault tree) shall be given for the probable faults with their remedial actions.	Check whether the Repair manual provided by the manufacturer covers the required aspects.
2.9	Mechanical standards The equipment shall be housed in a 19" rack up to 800 mm depth with front/back access or as per ETSI standard.	Physically inspect and record the observations.
2.10	Operating personnel safety requirements	
2.10.1	The equipment shall conform to IS 13252 part 1: 2010+Amd 2013+Amd 2015 "Information Technology Equipment – Safety- Part 1: General Requirements" [equivalent to IEC 60950-1:2005+A1:2009+A2:2013 "Information Technology Equipment –Safety- Part 1: General Requirements"]. The manufacturer/supplier shall submit a certificate in respect of compliance with these requirements.	Safety Report from TEC designated test lab to be submitted.
2.10.2	The optical access port shall be designed to protect itself against the entry dust when they are not occupied by an external fibre-optic connection. To prevent the failures in the optical line devices due to ingress of dust, the connectors provided at all high output devices shall be provisioned with the auto-shutter or shall be so positioned as facing downwards to avoid the direct incidence of laser-beam on the user. The optical access port shall be easy to clean by the user.	Physically inspect and record the observations.
2.10.3	The laser product shall meet the optical safety requirement as per IEC 60825-1. The equipment shall meet the optical safety requirement as per the Automatic Laser Shut Down (ALSD)/ Automatic Power Reduction (APR) procedure of ITU-T Rec. G.664 (latest edition) on Class B laser. The equipment shall have visual warnings and controls ensuring danger-free operation. Laser safety signs and instructions shall be mentioned in the QKD equipment. An undertaking/test certificate shall be sufficient during certification.	Undertaking/ Test Certificate to be submitted.
2.10.4	Protection against short circuits/open circuits in the access points shall be provided. All switches/controls on the front panel shall have suitable safeguards against accidental operations.	Physically inspect and record the observations.

2.10.5	The equipment shall have a terminal for grounding the rack.	Physically inspect and record the observations.
2.10.6	All switches/controls on the front panel shall have suitable safeguards against accidental operation.	Physically inspect and record the observations.
2.10.7	The equipment shall be adequately covered to safeguard against entry of even dust, insects, etc.	Physically inspect and record the observations.
2.11	**Minimum Equipment Requirement for Testing & Certification** Fully Equipped QKD Terminals are required in the following configurations: Receiver QKD Terminal : 01 No. Sender QKD Terminal : 01 No. Trusted Node : 01 No. Data path equipment : 02 Nos GUI (O&M) : 01 No. An Additional terminal will be required for Point to Multipoint QKD system testing. QKD system may be offered for TEC certification in any of the following configurations: i. P2P QKD system without Trusted Relay node ii. P2P QKD system with Trusted Relay node iii. QKD system with Star Topology iv. Multipoint QKD system	This is for information purpose.
2.12	**Field Trial** Post testing of equipment in the lab, the equipment shall be offered for test in the actual working environment. i. The QKD system (Point to Point(P2P) QKD System field trial may be done for a minimum of 4 weeks. ii. The QBER of the QKD system should not exceed 5%. iii. There should not be any impact on the normal working of conventional channels for data traffic.	Test Case No. 45
2.13	**Environmental Testing Requirement** It is understood that the QKD equipment shall be operated in IN/IC environment, accordingly following environmental tests are described for the equipment. In case requirements as given in the table below;	Report from TEC designated test lab to be submitted.

Table 2: Environmental Testing Requirement

S.No.	Environmental Tests	Temperature Conditions	Humidity Conditions
	Low Temp (Cold) Cycle	TOL: 10 °C TSL: 18 °C Ambient Temp: 20°C	NA
	High Temperature (Dry Heat) cycle	TOH: 25°C, TSH: 22°C. Ambient Temp: 20°C	NA
	Tropical Exposure (Damp Heat Cyclic)	Max Temperature during System OFF condition for all 4 days: 25 °C Ambient Temp: 20°C	Rh-95%
	Rapid Temperature Cycling Test	LST: 10 °C HST: 25°C. Ambient Temp: 20°C	NA
	Damp Heat (Steady State)	Max Temperature during System ON condition for all 4 days: 25°C Ambient Temp: 20°C	Rh-95%

	CHAPTER 3	
	Safety & EMC Requirements	
3.1	**Safety**	
3.1.1	The equipment shall conform to IS/IEC 62368-1:2023 "Audio/video, information and communication technology equipment as prescribed under Table no. 1 of the TEC document 'SAFETY REQUIREMENTS OF TELECOMMUNICATION EQUIPMENT": TEC10009: 2024".	Report from TEC accredited test lab to be submitted.

3.1.2	Laser safety: The equipment shall conform to IEC 60825-2:2021 for products emitting laser radiation and IEC 60825-2:2021 for optical fibre communication systems (OFCSs) as prescribed under Table no. 1 of the TEC document 'SAFETY REQUIREMENTS OF TELECOMMUNICATION EQUIPMENT": TEC10009: 2024". **Note:** This test shall be applicable if laser components are directly mounted in the box.	Report from TEC accredited test lab to be submitted.
3.2	**General Electromagnetic Compatibility (EMC) Requirements** The equipment shall conform to the EMC requirements as per the following standards and limits indicated therein. A test certificate and test report shall be furnished from an accredited test agency.	Report from TEC accredited test lab to be submitted.
3.2.1	**Conducted and radiated emission (applicable to telecom equipment):** **Name of EMC Standard:** "CISPR 32:2015+A1:2019 – Electromagnetic compatibility of multimedia equipment - Emission requirements" i. To comply with Class B of CISPR 32:2015+A1:2019. ii. For Radiated Emission tests, Limits below 1 GHz as per Table 4(a), 5(a),4 (a1) & 5 (a1) 1) **Table 4(a):** Limits for unwanted radiated emission of "Class B" equipment at a measuring distance of 10m. 2) **Table 5(a):** Limits for unwanted radiated emission of "Class A" equipment (for Telecommunication Centres) at a measuring distance of 10m. 3) **Table 4(a1):** Limits for unwanted radiated emission of class B Equipment at a measuring distance of 3 m. 4) **Table 5(a1):** Limits for unwanted radiated emission of class A Equipment at a measuring distance of 3 m. iii. For Radiated Emission tests, Limits above 1 GHz as per Table 4(b) & 5(b). 1) **Table 4(b):** Limits for radiated disturbance of class B Eqpt. at a measurement distance of 3 m. 2) **Table 5(b):** Limits for radiated disturbance of class A Eqpt.at a measurement distance of 3 m. OR **Conducted and radiated emission (applicable to instruments such as power meter, frequency counter, etc.):**	Report from TEC accredited test lab to be submitted.

	Name of EMC Standard: " CISPR 11 {2024} - Industrial, Scientific and Medical (ISM) radio-frequency equipment - Electromagnetic disturbance characteristics- Limits and methods of measurement". **Limits:** i. The applicable limits shall be for the category of Group 1 of class A type equipment. The same are reproduced in Tables 5 (a & b) & 7 for radiated & conducted disturbance respectively. 1) **Table 5(a):** Limits for unwanted radiated emission of "Class A" equipment (for Telecommunication Centres) at a measuring distance of 10m. 2) **Table 5(b):** Limits for radiated disturbance of class A Eqpt.at a measurement distance of 3 m. 3) **Table 7:** Limit of conducted emission (disturbance) at the main ports of Class A Telecom Equipment.	
3.2.2	**Immunity to Electrostatic discharge:** **Name of EMC Standard:** IEC 61000-4-2:2025 "Testing and measurement techniques of Electrostatic discharge immunity test". **Limits:** i. Contact discharge level 2 {± 4 kV} or higher voltage; ii. Air discharge level 3 {± 8 kV} or higher voltage; Performance Criteria shall be as per Table 1 under Clause 6 of TEC Standard No. TEC 11016:2016. Applicable Performance Criteria shall be as per Table 3 under Clause 7.2 of TEC Standard No. TEC 11016:2016.	Report from TEC accredited test lab to be submitted.
3.2.3	**Immunity to radiated RF:** **Name of EMC Standard:** IEC 61000-4-3 (2020) "Testing and measurement Techniques-Radiated RF Electromagnetic Field Immunity test". **Limits:** i. **For Telecom Equipment and Telecom Terminal Equipment with Voice interface (s)** 1) Under test level 2 {Test field strength of 3 V/m} for general purposes in the frequency range 80 MHz to 1000 MHz and	Report from TEC accredited test lab to be submitted.

	2) Under test level 3 (10 V/m) for protection against digital radio telephones and other RF devices in the frequency ranges 800 MHz to 960 MHz and 1.4 GHz to 6.0 GHz. ii. For Telecom Terminal Equipment without Voice interface (s) 1) Under test level 2 {Test field strength of 3 V/m} for general purposes in the frequency range 80 MHz to 1000 MHz and protection against digital radio telephones and other RF devices in the frequency ranges 800 MHz to 960 MHz and 1.4 GHz to 6.0 GHz. Performance Criteria shall be as per Table 1 under Clause 6 of TEC Standard No. TEC 11016:2016. Applicable Performance Criteria shall be as per Table 3 under Clause 7.2 of TEC Standard No. TEC 11016:2016.	
3.2.4	Immunity to fast transients (burst): Name of EMC Standard: IEC 61000- 4- 4 {2012) "Testing and measurement techniques of electrical fast transients / burst immunity test" Limits: i. Test Level 2 i.e., a) 1 kV for AC/DC power lines; b) 0. 5 kV for signal / control / data / telecom lines. Performance Criteria shall be as per Table 1 under Clause 6 of TEC Standard No. TEC 11016:2016. Applicable Performance Criteria shall be as per Table 3 under Clause 7.2 of TEC Standard No. TEC 11016:2016.r	Report from TEC accredited test lab to be submitted.
2.2.5	Immunity to surges: Name of EMC Standard: As per IEC 61000-4-5 (2014) "Testing & Measurement techniques for Surge immunity test" Limits: i. For mains power input ports: 1) 2 kV peak open circuit voltage for a line-to-ground coupling. 2) 1 kV peak open circuit voltage for a line-to-line coupling.	Report from TEC accredited test lab to be submitted.

	ii. For telecom ports: 1) 2 kV peak open circuit voltage for line to ground. 2) 2 kV peak open circuit voltage for line-to-line coupling. The performance criteria as given in clause 6 and as per Table 3 Immunity of Clause 7.2 of TEC Standard No. TEC 11016:2016 shall apply.	
3.2.6	Immunity to conducted disturbance induced by Radio frequency fields: Name of EMC Standard: IEC 61000-4-6 (2023) "Testing & measurement Techniques-Immunity to conducted disturbances induced by radiofrequency fields". Limits: i. Under the test level 2 {3Vr.m.s.}in the frequency range 150 kHz-80 MHz for AC / DC lines and Signal /Control/telecom lines. Performance Criteria shall be as per Table 1 under Clause 6 of TEC Standard No. TEC/SD/DD/EMC-221/05/OCT-16. Applicable Performance Criteria shall be as per Table 3 under Clause 7.2 of TEC Standard No. TEC/SD/DD/EMC-221/05/OCT-16.	Report from TEC accredited test lab to be submitted.
3.2.7	Immunity to voltage dips & short interruptions (applicable to only ac mains power input ports, if any): Name of EMC Standard: IEC 61000-4-11 (2020) "Testing & measurement techniques- voltage dips, short interruptions and voltage variations immunity tests" Limits: i. a voltage dip corresponding to a reduction of the supply voltage of 30% for 500ms (i.e., 70 % supply voltage for 500ms) ii. a voltage dip corresponding to a reduction of the supply voltage of 60% for 200ms; (i.e., 40% supply voltage for 200ms) iii. a voltage interruption corresponding to a reduction of a supply voltage of > 95% for 5s.	Report from TEC accredited test lab to be submitted.

	iv. a voltage interruption corresponding to a reduction of a supply voltage of >95% for 10ms. Performance Criteria shall be as per Table 1 under Clause 6 of TEC Standard No. TEC 11016:2016. Applicable Performance Criteria shall be as per Table 3 under Clause 7.2 of TEC Standard No. TEC 11016:2016.	
3.2.8	**Immunity to voltage dips & short interruptions (applicable to only DC power input ports, if any):** Name of EMC Standard: IEC 61000-4-29:2000: Electromagnetic compatibility (EMC) - Part 4-29: Testing and measurement techniques - Voltage dips, short interruptions and voltage variations on DC input power port immunity tests. Limits: i. Voltage Interruption with 0% of supply for 10ms. Applicable Performance Criteria shall be B. ii. Voltage Interruption with 0% of supply for 30ms, 100ms, 300ms and 1000ms. Applicable Performance Criteria shall be C. iii. Voltage dip corresponding to 40% & 70% of supply for 10ms, 30 ms. Applicable Performance Criteria shall be B. iv. Voltage dip corresponding to 40% & 70% of supply for 100ms, 300 ms and 1000 ms. Applicable Performance Criteria shall be C. v. Voltage variations correspond to 80% and 120%of supply for 100 ms to 10s as per Table 1c of IEC 61000-4-29. Applicable Performance Criteria shall be B. Note 1: Classification of the equipment: Class B: Class B is a category of apparatus which satisfies the class B disturbance limits. Class B is intended primarily for use in the domestic environment and may include: i. Equipment with no fixed place of use; for example, portable equipment powered by built in batteries; ii. Telecommunication terminal equipment is powered by telecommunication networks. iii. Personal computers and auxiliary connected equipment	Report from TEC accredited test lab to be submitted.

	Please note that the domestic environment is an environment where the use of broadcast radio and television receivers may be expected within a distance of 10 m of the apparatus connected. **Class A:** Class A is a category of all other equipment, which satisfies the class A limits but not the class B limits. **Note 2:** The testing agency for EMC tests shall be an accredited agency and details of accreditation shall be submitted. **Note 3:** For checking compliance with the above EMC requirements, the method of measurements shall be by TEC Standard No. TEC 11016:2016 (or latest release) and the references mentioned therein unless otherwise specified specifically. Alternatively, corresponding relevant Euro Norms of the above IEC/CISPR standards are also acceptable subject to the condition that frequency range and test level are met as per the above mentioned sub clauses 3.2.1 to 3.2.8 and TEC Standard No. 11016:2016 (or latest release). The details of IEC/CISPR and their corresponding Euro Norms are as follows: IEC/CISPR Euro Norm CISPR 11 EN 55011 CISPR 32 EN 55032 IEC 61000-4-2 EN 61000-4-2 IEC 61000-4-3 EN 61000-4-3 IEC 61000-4-4 EN 61000-4-4 IEC 61000-4-5 EN 61000-4-5 IEC 61000-4-6 EN 61000-4-6 IEC 61000-4-11 EN 61000-4-11 IEC 61000-4-29 EN 61000-4-29	
	CHAPTER 4	
4.1	Information for the procurer of product This chapter describes the requirements which may be included in the tender by the procurer as per its needs. The following items need to be specified by ordering authority depending upon the actual requirements:	For information of the procurer.
4.1.1	The procurer shall specify the required QKD configuration as provided below: 1) P2P QKD system without Trusted Relay node 2) P2P QKD system with Trusted Relay node 3) QKD system with Star Topology	For information of the procurer.

	4) Multipoint QKD system	
4.1.2	The procurer shall specify the Quantum Channel Loss and the range over which the QKD system to be deployed. The range of the QKD system may vary with Quantum Channel loss.	For information of the procurer.
4.1.3	QBER performance and Minimum Key Rate shall be as specified in table 1. QBER may increase and key rate may decrease for higher Quantum Channel loss. The same may be specified by the procurer, based on their requirements and considering the security aspects.	For information of the procurer.
4.1.4	The procurer may specify the dimensions of the Transmitter and Receiver unit.	For information of the procurer.
4.1.5	In case of tamper detection and security attack, the response of the QKD system may be specified by the manufacturer.	For information of the procurer.
4.1.6	The secure hardware implementation to store the generated keys may be specified by the procurer.	For information of the procurer.
4.1.7	The procurer based on its requirements for additional requirement for security may optionally specify the additional requirements.	For information of the procurer.
4.1.8	The procurer may specify the MTBF and MTTR requirements.	For information of the procurer.
4.1.9	The procurer may specify the alarms in the system for failure or in the event of eaves dropping.	For information of the procurer.
4.2	Specific items to be mentioned in the certificate The following details shall be mentioned on the certificate:	For information of the procurer.
4.2.1	Model number(s) of the system offered for testing along with the Hardware Version and Software Version.	For information of the procurer.
4.2.2	Configuration of the QKD System offered for Testing.	For information of the procurer.
4.2.3	Maximum Channel loss declared by the Manufacturer for P2P QKD link for which the system is certified.	For information of the procurer.

I. TEST SETUP & PROCEDURES:

Test Case No. 1

Functionalities of QKD System				
S.No.	Details	Test Procedure	Expected Output	Observations during Testing
1.	System Boot-up and Initialization	Power ON the QKD system and verify through the system logs and/or GUI status that the system has booted successfully, completed auto-calibration and synchronization procedures, and initiated key generation.	The QKD system shall boot successfully and perform auto-calibration /synchronization and thereafter, key generation shall be initiated.	
2.	Key Sifting	Verify through the system logs that the key sifting process is executed during key generation.	The QKD system shall successfully perform key sifting as part of the key generation process.	
3.	Error Estimation/Correction	1. Monitor the Quantum Bit Error Rate (QBER) through the GUI, logs, or diagnostic interface. 2. Obtain the final key file generated at Alice and Bob and compare them for consistency.	Key files generated at Alice and Bob shall be identical.	
4.	Privacy Amplification	Check the key size after error correction and	The final key length shall be reduced compared to	

		verify that the final key length is reduced according to the configured security parameters. Record the compression ratio.	the key length after error correction.	
5.	Key Management	Verify from the logs the storage and lifecycle management (Generation Timestamp, QKD module ID, Key length, etc,) of the generated keys. Request a key of 256-bit length through the key delivery interface at Alice. Using the corresponding Key ID, retrieve the key through the key delivery interface at Bob	The QKD system shall store the generated keys along with the associated key lifecycle information. 256-bit key requested at Alice shall be successfully retrieved at Bob using the corresponding Key ID, and the delivered keys shall be identical.	
6.	Monitoring of Performance and System Health Parameters	Verify through the GUI that performance and health parameters such as key rate, QBER, alarms, hardware status, etc. are available and updated during operation.	Performance and system health parameters of the QKD system can be monitored through the GUI	

Test Case No. 02

Sender Node Details				
S.No.	Details	Test Procedure	Expected Output	Observations during Testing
1.	Dimensions of Sender Node	Physically inspect the Sender (Alice) Node and measure its dimensions. Verify rack-mount compatibility.	The Alice Node should be 19'' Rack mountable with the height of size 1U/2U/3U, etc.	
2.	Type of Signal Source	Record the Type of Signal source and verify from the corresponding product datasheet of	The signal source shall be continuous wave laser/pulsed laser/ single photon source.	
3.	Wavelength of Signal Source	Using an optical spectrum analyzer, measure the wavelength at the output of the Alice Node on Quantum Channel	The wavelength shall be in the range from 1530nm to 1565 (C-band)	
4.	Modulation	Record the QKD protocol implemented in the Sender Node and verify the modulation characteristics of the transmitted optical signal using suitable test equipment.	The observed signal shall exhibit intensity modulation for the CoW protocol and phase modulation for the DPS protocol, as applicable.	
5.	g2(0) value	Measure $g^{(2)}(0)$ value of the source using an HBT setup. However, if the required measurement facilities	For a single photon source, the second-order correlation value g2(0) shall be <<1 and mentioned in the product datasheet. For a weak	

		are not available, verify the $g^{(2)}(0)$ value from the manufacturer's test report, or product datasheet in case the single-photon source is procured from a third-party manufacturer.	coherent source, the second-order correlation value g2(0) shall be ~1.	
6.	Type of Random Number Generator	Verify the operating principle of the Random Number Generator (RNG) implemented in the Sender Node through physical inspection and review of the manufacturer's documentation. If the RNG is used from a third-party manufacturer, verify its type from the corresponding product datasheet	The Random Number Generator used shall be a QRNG/TRNG.	

Test Case No. 03

Receiver Node Details				
S.No.	Details	Test Procedure	Expected Output	Observations during Testing
1.	Dimensions of Sender Node	Physically inspect the Receiver (Bob) Node and measure its dimensions. Verify rack-mount compatibility.	The Receiver Node should be 19'' Rack mountable with the height of size 1U/2U/3U, etc.	
2.	Type of Single Photon Detector	Record the type of Single Photon Detector (SPAD/ SNSPSD) implemented in the Receiver Node and verify the specifications from the corresponding product datasheet and technical documentation.	The Receiver Node shall have a Single Photon Detector for single photon detection.	
3.	Wavelength of Signal Photon Detector	Using an optical spectrum analyzer, measure the wavelength at the input of the Receiver Node on Quantum Channel. Verify that the Single Photon Detector registers photon detection events.	Single Photon Detector shall detect photons for wavelength on the quantum channel in the range from 1530nm to 1565nm.	
4.	Control Electronics	Configure the SPAD parameters eg. Efficiency, Dead Time, etc. and other system parameters through the GUI/command line	The other system parameters shall be successfully configured. For instance, Increase in efficiency would lead to increase in photon	

		interface. Verify that the corresponding changes in performance are observed.	detection efficiency and the key rate.	
5.	Type of Random Number Generator (if available)	Verify the operating principle of the Random Number Generator (RNG) implemented in the Sender Node through physical inspection and review of the manufacturer's documentation. If the RNG is used from a third-party manufacturer, verify its type from the corresponding product datasheet	The Random Number Generator used shall be a QRNG/TRNG.	

Test Case No. 04

Statistics of the QKD source				
S.No.	Details	Test Procedure	Expected Output	Observations during Testing
1.	Mean photon number (μ)	Measure the average optical power at the output of the Sender Node using an optical power meter. Using the pulse repetition rate (f) and operating wavelength (λ), calculate the average number of photons per pulse (μ) as	Mean photon number (μ) shall be less than 1.	

		$\mu = \frac{P_{\text{avg}}}{f}\left(\frac{\lambda}{hc}\right)$		
2.	Probability Distribution, p(n)	Perform photon statistics measurements to characterize and plot the photon number probability distribution, $p(n)$. Alternatively, if the required test facilities are not available, an undertaking / datasheet shall be submitted by the manufacturer regarding the probability distribution.	The photon number probability distribution p(n) shall be Poissonian for weak coherent source. For a single-photon source, the distribution shall demonstrate a probability of approximately 1 for single-photon emission.	

Test Case No. 05

Mean photon number				
S.No.	Details	Test Procedure	Expected Output	Observations during Testing
1.	Configuration of Mean photon number	1. Configure different mean photon number (μ) values through the GUI and/or management interface. 2. For each configured value, establish a QKD session and monitor the average key rate for three different values of μ: Key Rate [μ_1=0.1]: ___ Kbps	1. The QKD system shall allow successful configuration of different mean photon number (μ) values. 2. Average Key Rate shall increase on increasing the mean photon number.	

		Key Rate [μ_2=0.3]: ___ Kbps Key Rate [μ_3=0.5]: ___ Kbps		

Test Case No. 06

Single Photon Detector (SPD) Characteristics and Security Countermeasures				
S.No.	Details	Test Procedure	Expected Output	Observations during Testing
1.	SPAD Characteristics	Initiate the QKD system in the key generation state, and record the following characteristics of the Single photon detector from the system GUI and/or accessing the system through the management interface:		
		SPD Type:	Record the type of SPD used eg. SNSPD, SPAD, etc.	
		Mode of Operation:	Record the Mode of Operation of SPD: Gated/ Free Running	
		Dark count rate	< 800 counts per second	
		After Pulse rate	< 1% for free-running mode and <0.5% for Gated mode	
		Jitter	< 200 ps	
		Dead Time	< 100 µs	

Test Case No. 07

Countermeasures against quantum/classical channel attacks

S.No.	Details of Attack	Test Procedure	Expected Output	Observations during Testing
1.	Intercept and Resend Attack	Check whether proper authentication mechanism are implemented on the classical channel between Alice and Bob before the signal is transmitted on the Quantum Channel	The QKD nodes shall be authenticated before initiating the key generation.	
2.	Beam Splitter Attack	Insert an attenuator in the quantum channel to simulate the beam splitter attack.	The QKD system shall stop the key generation when QBER exceeds 5%.	
3	Detector Blinding Attack	The appropriate protocol parameters (eg. decoy states, mean photon number, etc.) and countermeasures implemented in the system to secure the system against these attacks to be submitted by the manufacturer.	The protocol parameters and countermeasures are implemented to ensure security against the attacks.	
4	Photon Number Splitting (PNS) Attack			
5	Coherent Attack			
6	Non-coherent Attack			
7	Other Attacks			

Test Case No. 08

Disclose Rate

<table>
<tr><th>S.No.</th><th>Details</th><th>Test Procedure</th><th>Expected Output</th><th>Observations during Testing</th></tr>
<tr><td>1.</td><td>Provision for changing disclose rate</td><td>1. Configure different disclose rate values through the GUI and/or management interface.
2. For each configured value, establish a QKD session and monitor the average key rate for three different values of disclose rate:<table><tr><th>Disclose Rate</th><th>Average Key Rate</th></tr><tr><td>[Value 1]</td><td></td></tr><tr><td>[Value 2]</td><td></td></tr><tr><td>[Value 3]</td><td></td></tr></table></td><td>1. The QKD system shall allow successful configuration of different values of disclose rate.
2. Average Key Rate shall decrease on increasing the disclose rate.</td><td></td></tr>
</table>

Test Case No. 09

<table>
<tr><td colspan="5">Privacy Amplification Rate</td></tr>
<tr><th>S.No.</th><th>Details</th><th>Test Procedure</th><th>Expected Output</th><th>Observations during Testing</th></tr>
<tr><td>1.</td><td>Provision for changing privacy amplification rate</td><td>1. Configure different privacy amplification rate values through the GUI and/or management interface.
2. For each configured value, establish a QKD session and monitor the average key rate for three different values of privacy amplification rate:</td><td>1. The QKD system shall allow successful configuration of different values of privacy amplification rate.
2. Average Key Rate shall decrease on increasing the disclose rate.</td><td></td></tr>
</table>

		Privacy Amplification Rate	Average Key Rate		
		[Value 1]			
		[Value 2]			
		[Value 3]			

Test Case No. 10

Information Reconciliation Algorithm				
S.No.	Details	Test Procedure	Expected Output	Observations during Testing
1.	Provision for changing Information Reconciliation Algorithm	1. Configure different Information Reconciliation algorithms through the GUI and/or management interface (if the feature is supported). 2. For each configured algorithm, establish a QKD session and verify that the keys are successfully being generated. 3. Monitor the average key rate and average QBER.	1. The QKD system shall allow successful configuration and selection of different Information Reconciliation algorithms, if supported. 2. Average QBER shall be less than 5% and the key rate shall be greater than as specified in clause 1.8.2. 3. The final keys fetched at Alice and Bob shall be identical.	

Information Reconciliation Algorithm	Average Key Rate	Average QBER
[Algorithm 1]		
[Algorithm 2]		

<table>
<tr><td></td><td></td><td>4. Request a key from Alice and retrieve the corresponding key from Bob. Compare the retrieved keys to verify that they are identical.</td><td></td><td></td></tr>
<tr><td>2.</td><td>Provision to change code rate of Information Reconciliation Algorithm</td><td>1. Configure different code rate values for the Information Reconciliation algorithm through the GUI and/or management interface.
2. For each configured code rate, establish a QKD session and record the following observations:
<table><tr><th>Code Rate</th><th>Average Key Rate</th><th>Average QBER</th></tr><tr><td>[Code Rate 1]</td><td></td><td></td></tr><tr><td>[Code Rate 2]</td><td></td><td></td></tr></table>
3. Request a key from Alice and retrieve the corresponding key from Bob. Compare the retrieved keys to verify that they are identical.</td><td>1. The QKD system shall allow successful configuration of different code rate values for the Information Reconciliation algorithm, if applicable.
2. Average QBER shall be less than 5% and the key rate shall be greater than as specified in clause 1.8.2 for the differen.t code rates.
3. The final keys fetched at Alice and Bob shall be identical.</td><td></td></tr>
</table>

Test Case No. 11

Management Interface				
S.No.	Details	Test Procedure	Expected Output	Observations during Testing

1.	Management Interface	Perform the following at both Alice and Bob nodes: 1. Connect a laptop with the management interface using a standard connector (eg. RJ-45 Ethernet, USB, or other supported interface) and access the local management interface and/or access the remote management interface from a remote workstation connected over the network. 2. Attempt to log in using invalid/incorrect credentials and verify that access is denied and an appropriate error message is displayed. 3. Verify successful login to the management interface using valid credentials. 4. Verify that the management interface provides access to configuration of system	Users with valid credentials are able to successfully log in and configure system parameters at both Alice and Bob nodes through the local and/or remote management interface.	

		parameters, logs, and status information.		

Test Case No. 12

Optical Connectors				
S.No.	Details	Test Procedure	Expected Output	Observations during Testing
1.	Optical Connector Interface	At both the Sender (Alice) and Receiver (Bob) nodes, perform the following: 1. Physically inspect the optical connector interfaces at and record the connector type (SC/LC/FC/ST). 2. Verify that the optical connectors shall have automatic shutters having spring action or provision of closing them manually. 3. Verify that when not in use, the optical connectors shall remain closed otherwise, the optical connectors are so	1. The optical connector is a standard connector type. 2. Automatic shutters with spring action or provision for manual closing are available on the optical connectors. 3. When not in use, the optical connectors shall remain closed or are positioned to avoid direct laser beam incidence on the user. 4. The optical return loss of the optical	

		positioned so as to avoid direct laser beam incidence on the user. 4. **Optical Return Loss:** Connect the optical return loss meter (or OTDR) to the optical connector using a standard patch cord. Record the optical return loss at the operating wavelength	connector shall be greater than 50 dB.	

Test Case No. 13

Random Number Generator – Clause 1.5.13				
S.No.	Details	Test Procedure	Expected Output	Observations during Testing
1.	**Statistical Testing of Random Number Generator**	1. Verify the operating principle of the Random Number Generator (RNG) implemented in the Sender & Receiver Node through physical inspection and review of the manufacturer's documentation/datasheet. 2. Collect 10^9 bits of data from the Random Number Generator.	1. The Random Number Generator used shall be a QRNG/TRNG. 2. The generated random bit sequences shall successfully pass the NIST SP 800-22 and Diehard Test suite.	

		3. Applying NIST statistical tests and Die Harder Tests on the collected data using the open-source software tools. 4. Verify that the obtained p-values are within the acceptance criteria specified by the respective test suites.		

Test Case No. 14

Details: The software/hardware in the equipment shall not pose any problem due to changes in date and time caused by events such as changeover of millennium/century, leap year etc. in the normal functioning of the equipment.

Test Procedure: Configure the system date and time to simulate the below scenarios. Verify Record the corresponding QKD system parameters (Average QBER and Average Key Rate) during the period of transition:

S.No.	Description	System Parameters over the Transition period	Interruption Observed in Key Generation during the period of transition (Yes/No)
QKD Protocol:			
1	Leap Year transition	Average QBER: Average Key Rate:	
2	Century/Millennium transition	Average QBER: Average Key Rate:	

Expected Output:

1. The QKD system continues normal operation without interruption.

2. The average QBER > 5% and average key rate shall be >1 Kbps for CoW protocol and > 2 Kbps for DPS protocol over the transition period.

Test Case No. 15

Authentication of QKD modules				
S.No.	Details	Test Procedure	Expected Output	Observations during Testing
1.	Authentication of QKD modules	1. Record the method used for authentication of QKD modules: — Pre-Shared Key Based Authentication — Digital Certificate Based — Any other 2. Initiate a session between Alice and Bob for key generation. Verify through logs that authentication is successfully completed over the classical channel prior to initiation of key generation. 3. Modify the configured authentication credentials (e.g., change the PSK , replace the digital certificate with an invalid/untrusted certificate, etc.) and restart the QKD system. Attempt to establish a QKD session and	1. The QKD modules shall successfully authenticate each other over the classical channel before initiation of key generation. 2. In case of invalid credentials, the authentication process shall fail and the QKD system shall not initiate key generation.	

		verify that authentication fails and key generation is not initiated.		

Test Case No. 16

Cryptographic security of Classical Channel				
S.No.	Details	Test Procedure	Expected Output	Observations during Testing
1.	Cryptographic security of Classical Channel	1. Record the cryptographic algorithms and the protocol as applicable (e.g., IPsec, TLS, SSH, etc.) used for securing the communication over classical channel. 2. Capture the classical channel traffic using a packet capture tool (e.g., Wireshark, tcpdump, etc.). 3. Verify from the pac capture the configured proto and the cipher suite used.	The classical channel between the QKD modules shall be secured using classical/ PQC Cryptographic algorithms.	

Test Case No. 17

Key Delivery Interface				
S.No.	Details	Test Procedure	Expected Output	Observations during Testing
1.	Key Delivery Interface	1. Request the key delivery from one QKD node using API	1. The QKD node shall successfully deliver the requested key	

		"Get key" as per ETSI GS QKD 014. Check whether the response is as per the '*Key Container data format*' specified in ETSI GS QKD 014. 2. Request key delivery from other QKD ndoe using API "Get key with key IDs" as per ETSI GS QKD 014. Check whether the response is as per the '*Key IDs data format*' specified in ETSI GS QKD 014. 3. Verify from the logs and record the other protocols supported by the system for key delivery as applicable (eg. Secure Key Integration Protocol (SKIP), etc)	through the **"Get Key"** API. The response shall conform to the "**Key Container data format"** specified in ETSI GS QKD 014. 2. The corresponding QKD node shall successfully deliver the requested key through the **"Get Key with Key IDs"** API. The response shall conform to the **Key IDs data format** specified in ETSI GS QKD 014. 3. The key retrieved using the **"Get Key with Key IDs"** API shall be identical to the key delivered through the **"Get Key"** API.	

Test Case No. 18

QBER Threshold Alram Indication				
S.No.	Details	Test Procedure	Expected Output	Observations during Testing

1.	QBER Threshold Alram Indication	1. Establish a QKD session between Alice and Bob. 2. Introduce attenuation in the quantum channel so to increase the QBER beyond 5%. 3. Verify that the alarm is generated on GUI and/or through visual indicators on the system. 4. Restore the normal channel conditions and verify the key generation is resumed.	1. Upon increase of the QBER beyond 5%, the QKD module shall generate an alarm to alert the user and stop key generation. 2. Upon restoration of normal channel conditions, the QKD system shall resume normal key generation operation.	

Test Case No. 19

Details: Key Life Cycle Management

Test Procedure:

1. Access the Key Manager through the management interface.
2. Request the key delivery from the Alice and Bob node.
3. Verify and record the following key life cycle management information is maintained by the Key Manager:

S.No.	Elements of Key life cycle management	Data Format	Observations [Available / Not available]
1	Key ID		
2	Key length		

3	QKD module ID		
4	Key generation timestamp		
5	Name of application/ID to which the key is supplied		
6	Key supply timestamp		

Expected Output:

The Key Manager shall maintain and provide access to key life cycle management information for the keys.

Test Case No. 20

Key Management Policy				
S.No.	Details	Test Procedure	Expected Output	Observations during Testing
1.	Key Management Policy	1. Request key delivery from the Alice node. 2. Using the application ID, request the corresponding key from the Bob. 3. After key supply, check the status of the supplied key in the Key Manager and verify whether the supplied key is retained or deleted from the key storage in accordance with the configured key management policy.	The status of the supplied key shall accurately reflect the configured key management policy: - If the key deletion policy is configured, the supplied key shall be deleted and not available in the key manager after delivery. - If the key preservation policy is configured, the supplied key shall remain available in key storage after key delivery.	

		4. Record the key management policy applied.		

Test Case No. 21

Authentication of Cryptographic Application				
S.No.	Details	Test Procedure	Expected Output	Observations during Testing
1.	Authentication of Cryptographic Application	1. Check and verify the authentication mechanisms used for authentication of the cryptographic application eg. Username/Password, Digital Certificate, etc. 2. Using invalid authentication credentials (e.g., incorrect password, invalid certificate, etc.), attempt to request keys through the key supply interface. Verify that the authentication attempt fails. 3. Using the valid credentials, make a key request from the cryptographic application through the key supply	1. The Key Manager shall authenticate cryptographic applications processing requests for key delivery. 2. Unauthorized access to the key supply interface shall be rejected. 3. The Key Manager shall successfully supply the requested number of keys to the authenticated cryptographic application through the key supply interface.	

		interface and verify that the authentication is successful and the number of keys requested are delivered to the application.		

Test Case No. 22

Tamper Event Detection and Logging				
S.No.	Details	Test Procedure	Expected Output	Observations during Testing
1.	Tamper Event Detection and Logging	1. Simulate a tamper event by opening the enclosure of both the QKD Sender and Receiver. 2. Verify that the QKD Sender and Receiver detects the tamper event and generates an alarm. 3. Access the logs through the management interface or through GUI, verify that the tamper event is logged with the timestamp.	1. QKD Sender and Receiver shall detect the tamper event and generate an alarm. 2. The tamper event shall be recorded in the system logs with the corresponding timestamp.	

Test Case No. 23

Details: Star Topology

Test Procedure:

1. Configure the system with one Bob node (Hub) and at least two Alice nodes connected in a star topology.
2. Record the distance and the channel loss for all the P2P links in the topology.
3. Configure the optical switching time for all the P2P links in the topology.
4. Verify that QKD keys are successfully generated between all the P2P links. Record the following observations:

Link	Distance	Channel Loss	Configured Time	Average QBER	Average Key Rate
Alice 1 – Bob					
Alice 2 - Bob					
Alice n - Bob					

5. Request key delivery from each of the Alice nodes and using the application ID, request the corresponding key from the Bob. Repeat the key delivery operation three times for each P2P link and verify that the keys delivered at the Alice and Bob nodes are identical.

Link	Key Delivery at Alice [Successful / Not Successful]	Key Delivery at Bob [Successful / Not Successful]	Whether Keys at Alice and Bob are identical (Yes/No)
Alice 1 – Bob			
Alice 2 - Bob			
Alice n - Bob			

6. Configure the optical switching time through the GUI and verify that the updated switching time is applied successfully during switching between the connected Alice nodes during key generation.

7. Configure the migration of the keys from Alice 1 to Alice 2 using Bob as the Relay Node. Verify through logs that the Bob performs key relay between Alice 1 and Alice 2

8. Request key delivery from Alice 1 and using the application ID, request the corresponding key from the Alice 2. Repeat three times and verify that the keys delivered at the Alice 1 and Alice 2 are identical.

Expected Output:

1. The system shall automatically switch between connected Alice nodes without manual intervention and the switching time shall be user configurable.
2. The keys shall be successfully generated between Bob and each connected Alice node with average QBER < 5% and average key rate > 1 Kbps for CoW protocol and >2 Kbps for DPS protocol.
3. The optical switching time shall be user-configurable and switching between connected Alice nodes shall occur automatically.
4. The Bob node shall successfully perform key relay between Alice nodes. The keys delivered at Alice 1 and Alice 2 through the key relay mechanism shall be identical.

Test Case No. 24

Online Performance Monitoring				
S.No.	Details	Test Procedure	Expected Output	Observations during Testing
1.	Online Performance Monitoring	1. Establish a QKD session between the QKD Sender and Receiver and ensure the keys are being generated. 2. Access the Local Craft Terminal (LCT), Element Management System (EMS), or management interface provided by the system for	1. The QKD module shall provide real-time monitoring of performance parameters through the LCT, EMS, and/or management interface. 2. The monitored parameter values shall be updated in real time during QKD operation.	

		performance monitoring. 3. Verify that the following parameters can be monitored in real time: - Quantum Bit Error Rate (QBER) - Key Rate - Mean Photon number (for weak coherent source) - SPD parameters like dead time, efficiency, etc.		
2.	On-demand Randomness Testing and Key Symmetry	1. Collect 10^{10} bits of secret key from both Alice and Bob Node. 2. Apply NIST statistical tests SP 800-22 on the collected data from Alice and Bob using the open-source software tools. 3. Verify that the obtained p-values are within the acceptance criteria. 4. Compare the key files and calculate ε-correctness of the key.	1. The final secret keys generated at both Alice and Bob nodes shall pass the applicable NIST statistical randomness tests. 2. The ε-correctness shall be less than 10^{-9}.	

Test Case No. 25

Details: Technical specifications of QKD system

Test Procedure:

Note down and record the following specifications as measured during the testing and/or specified by the manufacturer:

S.No.	Specification Description	Specified Value	Measured value /Observations
1	Secure Key Rate	>2Kbps for DPS protocol >1Kbps for COW protocol	<Record the average key rate at maximum Quantum Channel loss> In case of multi-point or P2P with relay node QKD systems, with more than one link, capture these parameters for each of those quantum peer links
2	QBER Value along with distance mentioned	<5%	<Record the average QBER at maximum Quantum Channel loss> In case of multi-point or P2P with relay node QKD systems, with more than one link, capture these parameters for each of those quantum peer links
3	Key transfer Interface	UART/USB/Ethernet	
4	Quantum Wavelength	C-Band @ITU-T DWDM grid	
5	Optical Return Loss	>50dB	

6	Fibre Type		G.652D, G.655, G.657			
7	Quantum Channel Loss for phase differential reference protocols	Type of the product	Short Range	Long Range	Extended Range	<Specify the range along with the Quantum Channel loss offered for certification. In case of multi-point or P2P with relay node QKD systems, with more than one link, capture these parameters for each of those quantum peer links >
		Application	<50 km	50-80 km	>80 km	
		Channel Loss	12dB	18dB	23dB	
8	Operating Temperature		10 to 25 °C			
9	Detector Type		SPD (SPAD / SNSPD)			
10	Power Supply		230V AC@50Hz or -48 V DC			
11	Mechanical Dimension of the rack		Width- 483 mm (19") Height- n*1U (1U ~ 45 mm) Depth - ≤ 800 mm Access - Front/back (Pizza box solution shall be mountable in a rack with the above dimensions)			
12	Synchronization (accuracy)		Over Classical Channel			

Expected Output:

The measured values and/or values for all applicable parameters shall conform to the technical specifications specified in the table

Test Case No. 26

Key re-size, key reformat

S.No.	Details	Test Procedure	Expected Output	Observations during Testing
1.	**Key re-size, and reformat**	1. Request a key of size greater than 8092 bits from Alice and retrieve the corresponding key from Bob. Verify that the keys are successfully delivered to Alice/ Bob and are identical. 2. Verify that appropriate key metadata (e.g., Key ID, generation time, key length) is maintained by the Key Manager.	1. The Key Manager shall successfully perform key re-size, reformat and storage to deliver a key of the requested length. 2. The Key Manager shall maintain the associated key metadata, including Key ID, generation time, key length, and other relevant attributes.	

Test Case No. 27

Functionality of Key Manager				
S.No.	Details	Test Procedure	Expected Output	Observations during Testing
1.	**Status information of QKD module(s) and QKD link(s) from the QKD module(s) in the quantum layer –** Clause 1.10.3	Check that the status information is received/maintained by the Key Manager, including QKD module status, QKD link status, key generation status, QBER, key rate, alarms, and fault conditions, as applicable.	The Key Manager shall maintain status information of the associated QKD module(s) and QKD link(s), or the information shall be available in the network control layer in SDN-based implementations.	

		In SDN-based deployments, verify that the status information is available in the network control layer.		
2.	**Key management information to the QKDN Controller** – Clause 1.10.4	1. Perform key relay operation between two QKD nodes. 2. Verify that the Key Manager (KM) provide information on key management for QKDN control/management functions to the QKDN controller. 3. Record the information provided by the Key Manager to the QKDN controller.	The Key Manager shall provide the required key management information to the QKDN Controller.	
3.	**Fault and performance information to the QKDN Manager** – Clause 1.10.5	1. Introduce a fault condition such as QKD link failure, KM link failure, etc. 2. Verify that the fault information is reported to the QKDN Manager. 3. Also, verify the availability of performance parameters such as key generation rate,	The Key Manager shall successfully report fault and performance information of the Key Manager and Key Manager links to the QKDN manager.	

		QBER, QKD Link status, etc. at the QKDN Manager.		
4.	**Key synchronization, entity authentication and message authentication for secure key relaying –** Clause 1.10.8	1. Initiate key relay between two key Managers and verify that the key is successfully relayed, synchronized and available at the receiving Key Manager. 2. Verify that the channel over which the key is relayed is secured using cryptographic algorithms or other appropriate security mechanisms.	1. Keys shall be successfully relayed between the communicating Key Managers. 2. The key relay channel is secured using cryptographic algorithms or other appropriate security mechanisms, as applicable.	

Test Case No. 28

Secure Hardware Implementation for Key Storage				
S.No.	Details	Test Procedure	Expected Output	Observations during Testing
1.	**Secure Hardware Implementation for Key Storage**	1. Record the mechanism for securing the storage of key in the QKD system. 2. Verify that the stored keys can only be	1. Generated Keys shall be securely stored in the QKD system. 2. Any unauthorized attempt to access the keys shall be denied.	

		accessed by the authorized entity.		

Test Case No. 29

Functionality of QKDN Controller				
S.No.	Details	Test Procedure	Expected Output	Observations during Testing
1.	**Key Relay Route Control and Rerouting –** Clause 1.11.1 and 1.11.3	1. Establish key relay between two KMs under the control of the QKDN Controller. 2. Request key delivery from the two KMs using the key delivery interface and verify successful key establishment. 3. Simulate a failure of an QKD link/KM Link and eavesdropping event on QKD Link in the active route between two KMs. 4. Verify that the QKDN Controller reroutes the key relay path through an alternate route. 5. Request key delivery again and verify successful end-to-end key establishment through the rerouted path.	1. The QKDN Controller shall establish and control the key relay route between the two Key Managers. 2. Upon failure of a Key Manager link, the QKDN Controller shall automatically reroute the key relay path through an alternate available route.	

2.	**Fault, performance, accounting, and configuration information to QKDN Manager –** Clause 1.11.4	1. Check that the fault, performance, accounting, and configuration information is maintained by the QKDN manager. 2. Introduce a fault condition such as QKD link failure, KM link failure, etc. 3. Verify that the fault information is available at the QKDN manager.	The QKDN controller shall provide fault, performance, accounting, and configuration information to a QKDN manager.	
3.	**Authentication and Authorization Control -** Clause 1.11.5 and 1.11.9	1. Add a functional element (eg. QKD module, Key Manager, etc.) in the QKD network. Verify that the functional element is successfully authenticated before being admitted to the network. 2. Disable a QKD link from the QKDN controller and verify that the key generation over the link is stopped.	1. The QKDN controller shall control the functional elements in the QKD network. 2. The QKDN Controller shall support authentication and access control of functional elements in the quantum layer and the key management layer.	
4.	**Charging Policy Control –** Clause	1. If supported, configure a charging policy.	The QKDN Controller shall apply charging policies as	

	1.11.6	2. Generate key distribution activity. 3. Verify policy application through logs, reports, etc.	configured, if supported.	
5.	**Quality of Service (QoS) Policy Control –** Clause 1.11.8	1. If supported, configure QoS policy parameters like Key Rate, QBER Threshold, Priority, etc. 2. Generate multiple service requests by changing the policy parameters. 3. Verify the QoS policies are applied.	The QKDN Controller shall apply configured QoS policies, if supported.	

Test Case No. 30

Functionality of QKDN Manager				
S.No.	**Details**	**Test Procedure**	**Expected Output**	**Observations during Testing**
1.	**Performance and Fault Management –** Clause 1.12.1, 1.12.2, 1.12.8, 1.12.9, 1.12.10, 1.12.12, 1.12.13 and 1.12.27	1. Verify that status information regarding Quantum Layer, Key Management Layer, and QKDN Controller is available at the QKDN manager. 2. Generate fault conditions such as QKD link failure, KM link failure, etc.	1. The QKDN Manager shall successfully collect and receive status information from the Quantum Layer, Key Management Layer, and QKDN Control Layer. 2. The generated fault conditions are correctly reported at	

		3. Verify that the fault information is available at the QKDN manager.	the QKDN Manager.	
2.	**Resource Management and Topology Management –** Clause 1.12.3, 1.12.5, 1.12.6, 1.12.7, 1.12.19, 1.12.20, 1.12.26 and 1.12.28	1. Access topology view of QKDN through the GUI. 2. Add an element QKD module, QKD link, Key Manager, etc. 3. Verify from GUI/logs that the resource is successfully added to the network and is operational. 4. Delete a functional element eg. QKD module, QKD link, Key Manager, etc. 5. Verify from GUI/logs that the resource is successfully removed and is no longer operational or accessible.	The QKDN Manager shall support configuration and management of resources. The network topology shall be updated upon addition or removal of functional elements.	
3.	**Resource Discovery and Bootstrapping –** Clause 1.12.11	1. Add a new QKD module. 2. Verify automatic or manual discovery and initialization operation. 3. Verify that key generation is	1. The QKDN Manager shall automatically or manually discover and register newly added QKD resources. 2. The discovered resource shall be successfully initialized.	

		successfully established following initialization.		
4.	**Accounting Management –** Clause 1.12.11	Verify that the QKDN Manager maintains the corresponding usage and accounting information (e.g., quantum key consumption, key relay, etc.).	Resource usage data shall be maintained by the QKDN manager.	
5.	**Key Supply Service Policy Management –** Clause 1.12.14 and 1.12.31	1. Configure a valid Key Supply Service Policy eg. minimum key size, maximum key size, application priority, etc. 2. Verify that the policy is enforced during key supply operations.	The QKDN Manager shall support configuration and management of Key Supply Service Policies.	
6.	**Logging of Security Anomalies –** Clause 1.12.15, 1.12.23 and 1.12.27	1. Simulate security-related events - eavesdropping attempt causing an abnormal QBER. 2. Verify that the QKDN Manager records the event in audit logs. 3. Also, verify detection and reporting of security anomalies.	The QKDN Manager shall successfully log the security-related events with relevant event details for traceability and analysis.	
7.	**Root CA and Access Control Support –** Clause 1.12.17	1. Issue a root certificate to the QKDN	1. The root certificate is successfully generated and signed. 2. Access control policies	

		Controller through the QKDN Manager. 2. Configure role based access control policies for the QKDN functional elements. 3. Attempt authorized and unauthorized access of the functional elements.	shall be successfully configured and enforced for the QKDN functional elements. 3. Authorized access requests shall be permitted and unauthorized access requests shall be denied.	
8.	**Key Management Policy –** Clause 1.12.18	1. Configure key management policies (e.g., key lifetime, key storage policy - expiry/preservation on delivery, etc). 2. Verify that the policies are successfully applied.	The QKDN Manager shall support management of key management policies.	
9.	**Authentication, Authorization and Multi-Factor Authentication (MFA) –** Clause 1.12.21 and 1.12.29	1. Register a QKDN element and assign access rights through the QKDN Manager. 2. Attempt access using an valid/invalid credentials and verify successful authentication and authorization 3. Verify that multi-factor authentication (MFA) is enforced for administrative and	1. The QKDN Manager shall authenticate and authorize management access, including module registration and access rights management. 2. QKDN manager shall enforce MFA for all administrative and privileged user access.	

		privileged user accounts using two or more authentication factors (e.g., password + Captcha, password + biometric, password + OTP, etc.), as applicable. 4. Attempt login using valid credentials and the required additional authentication factor. Verify the successful access. 5. Attempt login with valid credentials but without the additional authentication factor or with an invalid factor. Verify that the access request is denied.		
10.	QoS Management and Charging Management – Clause 1.12.22	QoS Management: 1. If supported, Configure a QoS policy (e.g., high priority for key delivery traffic). 2. Verify that the configured QoS policy is enforced during network operation, as applicable. Charging Management:	The QKDN manager may provide QoS management and charging management.	

		1. Perform QKDN operations involving key generation, key relay, or key consumption. 2. Verify that the QKDN Manager records the corresponding charging information, as applicable.		
11.	**Availability and Reliability through QKD Link Redundancy –** Clause 1.12.24 and 1.12.25	1. Establish key between two QKD nodes. 2. Simulate a failure of the active QKD link. 3. Verify that key distribution continues over the redundant QKD link or through an alternate key relay route, as applicable.	The key distribution is successfully maintained through a redundant QKD link or an alternate key relay route following failure of the active QKD link, as applicable.	
12.	**Role Assignment and Audit Logging -** Clause 1.12.30	1. Access the role management function provided by the QKDN Manager. 2. Create a new user and assign an appropriate role and permissions. 3. Modify and delete the assigned role permissions. 4. Verify that all role and permission changes are	The QKDN Manager shall provide a secure and auditable interface for role management, and all changes to roles and permissions shall be logged with the timestamp and user ID.	

		recorded in the audit logs along with the timestamp.		
13.	**Multi-Controller Orchestration and Management -** Clause 1.12.32	Verify that the QKDN Manager can monitor and manage multiple connected QKDN Controllers through a centralized management interface, if possible. Otherwise, an undertaking to be submitted by the manufacturer.	The QKDN Manager shall support orchestration, monitoring, and management of multiple QKDN Controllers, providing a unified view and centralized control across managed QKDN domains.	

Test Case No. 31

Common Data Models for Telemetry				
S.No.	Details	Test Procedure	Expected Output	Observations during Testing
1.	**Common Data Models for Telemetry**	1. Capture telemetry data from the Quantum Layer, Key Management Layer, and QKDN Control Layer. 2. Verify that quantum-layer metrics (e.g., QBER, photon count, key rate), KM metrics (e.g., secure-key balance, key consumption rate), and control-layer	The QKDN shall represent telemetry information using common data models for quantum-layer metrics, KM metrics, and control-layer status information.	

		status information are represented using the common data model e.g., YANG,JSON etc., as supported by the system.		

Test Case No. 32

Automatic Authentication and Operation on Reboot				
S.No.	Details	Test Procedure	Expected Output	Observations during Testing
1.	Automatic Authentication and Operation on Reboot	1. Reboot a QKD node and verify that all QKD nodes are automatically authenticated and restored to operational status without manual intervention. 2. Modify the authentication credentials (eg. certificate, etc.) of any QKD node and verify that authentication of the QKD node fails and an appropriate	1. The QKDN shall automatically authenticate and resume operation of the rebooted QKD nodes. 2. Authentication failures shall be detected and reported.	

		error/alarm is generated.		

Test Case No. 33

Unique Identifier for QKD Link				
S.No.	Details	Test Procedure	Expected Output	Observations during Testing
1.	**Unique Identifier for QKD Link**	1. Record the unique identifier is assigned to each QKD link in the QKDN. **QKD Link** | **Unique ID** | | | | | | 2. Verify that the identifier is used for key routing operations.	Each QKD link shall be assigned a unique identifier, which shall be used for key routing.	

Test Case No. 34

Cryptographic security of communication interface between QKD Module, QKDN controller and QKDN manager				
S.No.	Details	Test Procedure	Expected Output	Observations during Testing
1.	**Cryptographic security of**	1. Record the cryptographic	The communication interface between the QKD	

	communication interface between QKD Module, QKDN controller and QKDN manager	algorithms and protocols (e.g., TLS, IPsec, SSH, PQC-based protocols, etc.) used for securing the communication interface between the QKD Module, QKDN Controller, and QKDN Manager. 2. Capture the communication traffic between the QKD Module, QKDN Controller, and QKDN Manager using a packet capture tool (e.g., Wireshark, tcpdump, etc). 3. Verify from the packet capture the configured protocol and cipher suite used to secure the communication interfaces.	Module, QKDN Controller, and QKDN Manager shall be secured using Classical or Post-Quantum Cryptographic algorithms.	

Test Case No. 35

Redundancy of QKDN Controller and QKDN Manager				
S.No.	Details	Test Procedure	Expected Output	Observations during Testing

1.	**Redundancy of QKDN Controller and QKDN Manager**	1. Verify normal operation of the QKDN Manager and QKDN Controller. 2. Simulate failure of the active instance and verify failover to the standby instance (for Active-Standby) or continuity of service through other active instances (for Active-Active). 3. Verify that management and control functions continue without service interruption.	The QKDN Manager and QKDN Controller shall support a High Availability (HA) deployment architecture to ensure continuous operation through either Active-Standby or Active-Active deployment modes.	

Test Case No. 36

Dual-Stack IPv4/IPv6 Support				
S.No.	Details	Test Procedure	Expected Output	Observations during Testing
1.	**Dual-Stack IPv4/IPv6 Support**	1. Configure IPv4 / IPv6 address, as applicable. 2. Verify that management and service access are available over IPv4 / IPv6, as supported by the equipment.	The equipment successfully supports management and service accessibility over the configured IPv4 and/or IPv6 protocol stack(s), as applicable.	

		3. If dual-stack operation is supported, configure both IPv4 and IPv6 simultaneously and verify that management and service access are available over both IPv4 and IPv6.		

Test Case No. 37

Details: Service provisioning and system initialization procedure

Test procedure: Verify the procedure for service provisioning and system initialization for a multi-point QKD system, as per the clause 1.13.1 and record the observations.

> ***Note:*** *The signalling flow or sequence may vary depending on the implementation; however, the functionality shall conform to the requirements specified in the given clause.*

Expected Output: The QKDN controller, KM, and QKD modules are successfully initialized and configured as per the provisioning information.

Test Case No. 38

Details: Key generation procedure

Test procedure: Verify the key generation procedure in multi-point QKD system, as per the clause 1.14 and record the observations.

> ***Note:*** *The signalling flow or sequence may vary depending on the implementation; however, the functionality shall conform to the requirements specified in the given clause.*

Expected Output:

1. QKD modules shall push up the generated keys to KMs.
2. The KMs shall report the status of key generation to the QKDN controller and the QKDN manager.
3. The QKDN manager may optionally send supporting information to the QKDN controller.
4. The QKD module shall stop key generation upon receiving the request.

Test Case No. 39

Details: Key supply upon request mode

Test procedure: Verify the signaling procedures for key supply upon request mode implemented by two QKD nodes in a multipoint QKDN system, as per the clause 1.15 and record the observations.

> ***Note:*** *The signalling flow or sequence may vary depending on the implementation; however, the functionality shall conform to the requirements specified in the given clause.*

Expected Output: The keys are successfully delivered at the Source and Destination Cryptographic Application and are identical.

Test Case No. 40

Details: Proactive key supply mode

Test procedure: Verify the signalling messages request and the corresponding response received between the nodes of a multi-point QKD system, as per the clause 1.16 and record the observations.

> ***Note:*** *The signalling flow or sequence may vary depending on the implementation; however, the functionality shall conform to the requirements specified in the given clause.*

Expected Output: The keys are successfully delivered at the Source and Destination Cryptographic Application and are identical.

Test Case No. 41

A. **Note:** Either option 'A" or 'B' shall be verified as per the implementation by the manufacturer.**Details:** Key relay for a distributed QKDN

Test procedure: Verify the signalling procedures for key relay for a distributed QKDN, as per the clause 1.17 and record the observations.

> ***Note:*** *The signalling flow or sequence may vary depending on the implementation; however, the functionality shall conform to the requirements specified in the given clause.*

Expected Output: The keys shall be successfully relayed from KM1 to KM3.

B. **Details:** Key relay for a centralized QKDN

Test procedure: Verify the signalling procedures for key relay for a centralized QKDN with key reservation, as per the clause 1.17 and record the observations.

> ***Note:*** *The signalling flow or sequence may vary depending on the implementation; however, the functionality shall conform to the requirements specified in the given clause.*

Expected Output: The keys shall be successfully relayed from KM1 to KM3.

Test Case No. 42

Note: Either option 'A" or 'B' shall be verified as per the implementation by the manufacturer.

A. **Details:** Key request, key relay, and key supply for distributed QKDN

Test procedure: Verify the signalling procedures for key request, key relay, and key supply for a distributed QKDN, as per the clause 1.18.1 and record the observations.

> ***Note:*** *The signalling flow or sequence may vary depending on the implementation; however, the functionality shall conform to the requirements specified in the given clause.*

Expected Output: The keys are successfully relayed from KM1 to KM3 and identical keys are delivered at the Source and Destination Cryptographic Application.

B. **Details:** Key request, key relay, and key supply for centralized QKDN

Test procedure: Verify the signalling procedures for key request, key relay, and key supply for centralized QKDNs, as per the clause 1.18.2 and record the observations.

Note: *The signalling flow or sequence may vary depending on the implementation; however, the functionality shall conform to the requirements specified in the given clause.*

Expected Output: The keys are successfully relayed from KM1 to KM3 and identical keys are delivered at the Source and Destination Cryptographic Application.

Test Case No. 43

Details: Fault Alarm Generation

Test Procedure:

Note down the defined alarms in the system. Introduce or simulate faults in different system modules/units and monitor the alarm system.

S.No.	Alarm Description	Failure Simulated (Yes/No)	Alarm generated (Yes/No)	Monitoring (GUI/Hardware)

Expected Output: Appropriate alarms are generated and displayed on the QKD System GUI / hardware for each induced fault.

Test Case No. 44

Voltage Variation and Reverse Polarity Protection in case of DC feeds				
S.No.	Details	Test Procedure	Expected Output	Observations during Testing
1.	**Voltage Variation and Reverse**	1. Operate the QKD system within the	1. The equipment shall operate over the	

	Polarity Protection for DC feeds	specified nominal voltage range. 2. Vary the input voltage and frequency within the allowable operating range declared by the manufacturer and observe system performance. 3. Apply voltage beyond the specified range and verify that the system is protected and no damage or malfunction occurs. Check normal operation shall resume when correct voltage within the allowable range is restored. 4. Apply reverse polarity to the DC input (where applicable) and verify that the system is protected and no damage or malfunction occurs.	specified voltage range without any performance degradation. 2. The equipment shall be protected against voltage variations beyond the specified range.	

Test Case No. 45

Details: Field Trial

Test Procedure:

1. Deploy the P2P QKD system in the actual working environment at the distance offered for certification.
2. Operate the QKD system continuously for a minimum period of 4 weeks.
3. Monitor and record the below system parameters over the period of Field Trial:

S.No.	Parameters	Values during field Trial	Remarks
1	Average QBER (%)		Shall not exceed 5%.
2	Average Key Rate		> 1 Kbps for CoW protocol and > 2Kbps for DPS protocol
3	Visibility (for COW protocol)		> 90%
3	Link Availability (%)		Record the reasons for the duration for which the link was not available.
4	Impact on Conventional Data Traffic		Yes/No
5	Critical Alarms / Fault events generation		Record alarms, fault type, and corrective actions taken.
6	Key Delivery		Successful / Not successful

Expected Output: The P2P QKD system shall operate continuously in the actual working environment for a minimum period of four weeks with the specified performance requirements, including QBER and key generation rate and without any impact on the normal working of conventional channels for data traffic.

J. SUMMARY OF TEST RESULTS

TEC Standard No. TEC 91030:2026

TEC Test Guide No. TEC 91031:2026

Equipment name & Model No. 1. _____ 2. _____

Clause No.	*Compliance* *(Complied /Not Complied / Submitted/Not Submitted / Not Applicable)*	*Remarks /* *Test Report Annexure No.*

Date:

Place: Signature & Name of TEC testing officer/

*Signature of Applicant/ Authorized Signatory