Template for submitting comments/inputs on Draft Revision of GR on "QUANTUM KEY DISTRIBUTION SYSTEM" (Draft GR TEC 91000:2026)

Name of Manufacturer/Stakeholder:

Organization:

Contact details:

Clause No.	Clause Description	Proposed Revision	Justification

Note: The comments/inputs on the on Draft Revision of GR on "QUANTUM KEY DISTRIBUTION SYSTEM" (Draft GR TEC 91000:2026) may be furnished in the above format through email adgqt.tec-dot@gov.in with copy to adgtc2-tec-dot@gov.in at the earliest and within prescribed time period.

Template

सत्यमेव जयते

वर्गीय अपेक्षाएँ ~~आवश्यकताओं~~ के लिए मानक

दस्तावेज़ सं: टी.ई.सी. 91000:~~2022~~2026

STANDARD FOR GENERIC REQUIREMENTS

No. TEC 91000:~~2022~~2026 (DRAFT)

क्वांटम कुंजी वितरण प्रणाली

Quantum Key Distribution System

ISO 9001:2015

दूरसंचार अभियांत्रिकी केंद्र

खुर्शीदलाल भवन, जनपथ, नई दिल्ली-110001, भारत
TELECOMMUNICATION ENGINEERING CENTRE
KHURSHIDLAL BHAWAN, JANPATH, NEW DELHI–110001, INDIA
www.tec.gov.in

Release ~~1~~2: ______ ~~October~~, 2026~~2~~

FOREWORD

Telecommunication Engineering Centre (TEC) functions under the Department of Telecommunications (DOT), Government of India. Its activities include:

- Issue of Generic Requirements (GR), Interface Requirements (IR), Service Requirements (SR) and Standards for Telecom Products and Services
- Field evaluation of products and Systems
- National Fundamental Plans
- Support DOT on technology issues
- Testing & Certification of Telecom products

For testing, four Regional Telecom Engineering Centres (RTECs) have been established which are located in New Delhi, Bangalore, Mumbai, and Kolkata.

ABSTRACT

This document describes the generic requirements and specifications for Quantum Key Distribution (QKD) systems ~~as per, ITU-T Y.3801-3804 Recommendations~~ for use in the Indian telecom network.

Table of Content

HISTORY SHEET

S. No.	Name of the Standard	No. of the Standard	Remarks
1	Generic Requirements of the Quantum Key Distribution (QKD) System	TEC 91000:~~2022~~2026	~~First issue~~Draft
2	Generic Requirements of the Quantum Key Distribution (QKD) System	TEC 91000:2022	First issue

REFERENCES

S.No.	*Standard No.*	*Title*
1.	ITU-T Y.3800	Overview of networks supporting quantum key distribution
2.	ITU-T Y.3801	Functional requirements for quantum key distribution networks
3.	ITU-T Y.3802	Quantum key distribution networks - Functional architecture
4.	ITU-T Y.3803	Quantum key distribution networks - Key management
5.	ITU-T Y.3804	Quantum key distribution networks - Control and management
6.	ITU-T Y.4160	Quantum key distribution networks - Protocol framework
6.	ITU- T G.652	Characteristics of a single-mode optical fibre and cable
7.	ITU-T G.655	Characteristics of a non-zero dispersion-shifted single-mode optical fibre and cable
8.	ITU-T G.657	Characteristics of a bending-loss insensitive single-mode optical fibre- and cable
9.	ITU_T G.694.1	Spectral grids for WDM applications: DWDM frequency grid
10.	ETSI GS QKD 014	Protocol and data format of REST based Key Delivery API
11.	ETSI GS QKD 015	Quantum Key Distribution (QKD); Control Interface for Software Defined Networks

12.	ETSI GS QKD 016	Quantum Key Distribution (QKD); Common Criteria Protection Profile - Pair of Prepare and Measure Quantum Key Distribution Modules
13.	ETSI GS QKD 018	Quantum Key Distribution (QKD); Orchestration Interface for Software Defined Networks
14.	ETSI GS QKD 004	Quantum Key Distribution (QKD); Application Interface
15.~~11.~~	ETSI GR QKD 003	Components and Internal Interfaces
16.~~12.~~	ETSI 300	Equipment Engineering
17~~13.~~	NIST SP 800-90	Recommendation for Random Number Generation Using Deterministic Random Bit Generators00200
18~~14.~~	TEC/SD/DD/EMC-221	Electromagnetic Compatibility Standard for Telecommunication Equipment
~~1915.~~	~~QM-115~~	~~BSNL-QA document on Reliability Methods and Predictions~~
~~20~~19~~16.~~	ISO 9001:2015	Quality management system
20~~117~~	ISO/IEC DIS 23837-1	Information technology security techniques — Security requirements, test and evaluation methods for quantum key distribution — Part 1
21~~218~~	ISO/IEC DIS 23837-2	Information technology security techniques — Security requirements, test and evaluation methods for quantum key distribution — Part 2
22~~319~~	IEC 60825-1	Safety of laser products - Part 1: Equipment classification and requirements
23~~420~~	IEC 60825-2	Safety of laser products - Part 2: Safety of optical fibre communication systems (OFCSs)

Note:

Unless otherwise explicitly stated, the latest approved issue of the documents referred to above, with all amendments in force, on the issuance date of this GR shall be applicable.

CHAPTER-1

Technical Requirements

1.1 Introduction to QKD Technology

1.1.1 This document describes the generic requirements and specifications for Quantum Key Distribution (QKD) system ~~as per ITU-T Y.3800-3804 Recommendations~~ for use in the Indian telecom network. This document covers QKD protocols under differential 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.

1.1.2 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.

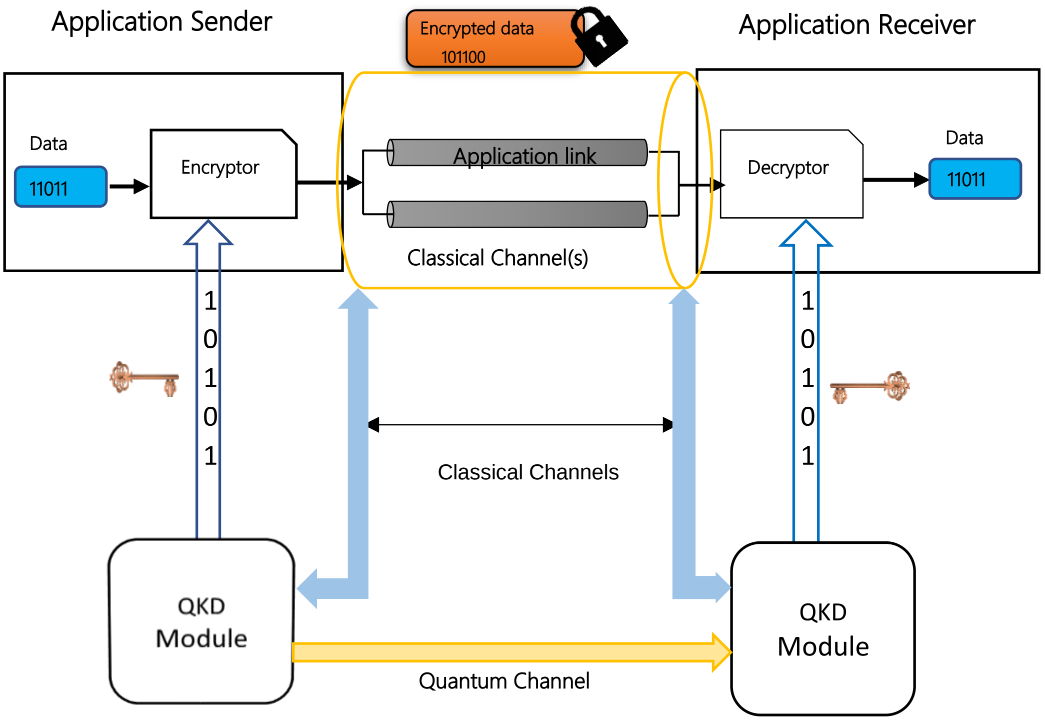


Figure 1 P2P QKD System

1.1.3 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 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.

1.1.4 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.

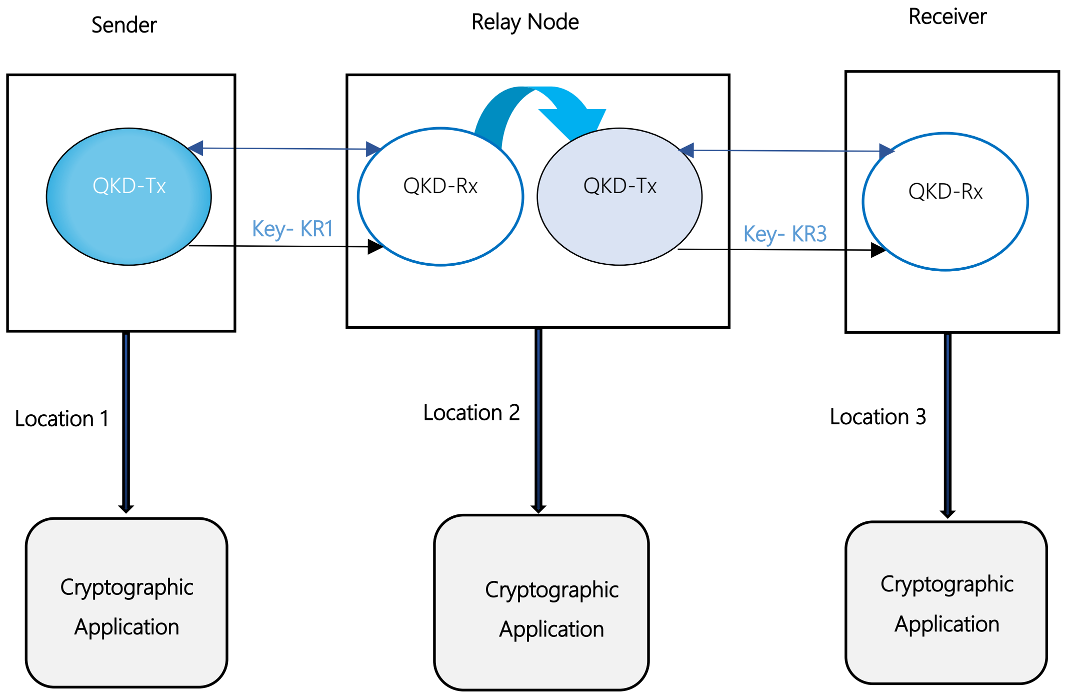


Figure 2 P2P QKD System with Relay Node

The operating principle of the trusted relay P2P QKD system shown above is explained below.

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 a 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 ~~must~~may be ~~capable of being~~ configured as an edge node.

1.1.5 Network Topologies for ~~P2P~~ QKD System:

A. 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.

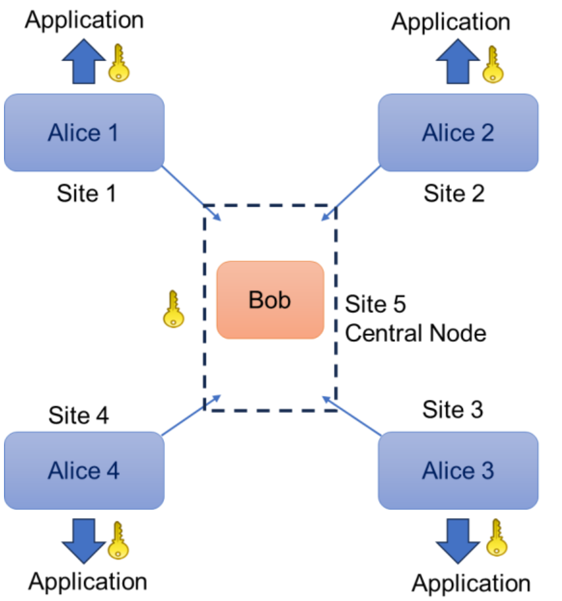


Figure 3A: Star QKD network topology

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.

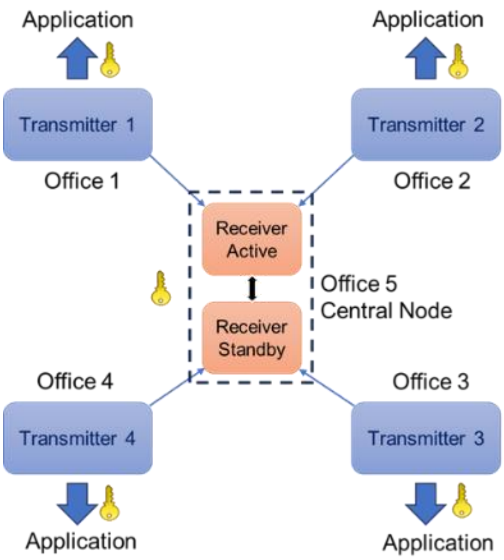


Figure 3B: Failsafe dual-star QKD network topology

B. 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 cyptographic applications through alternate relayed path.

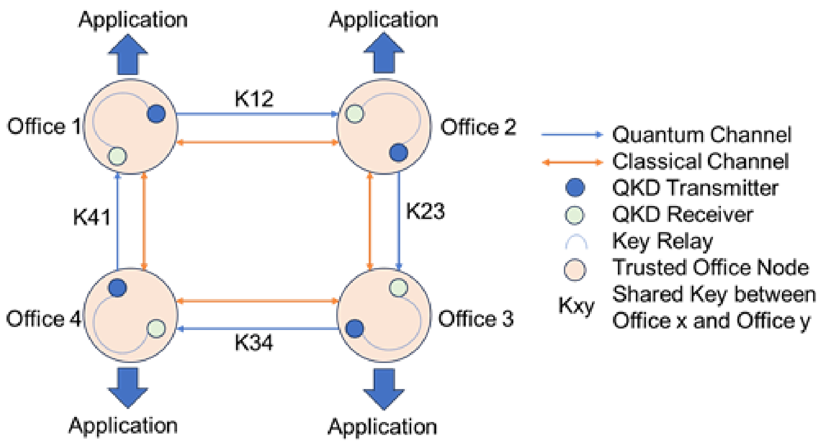
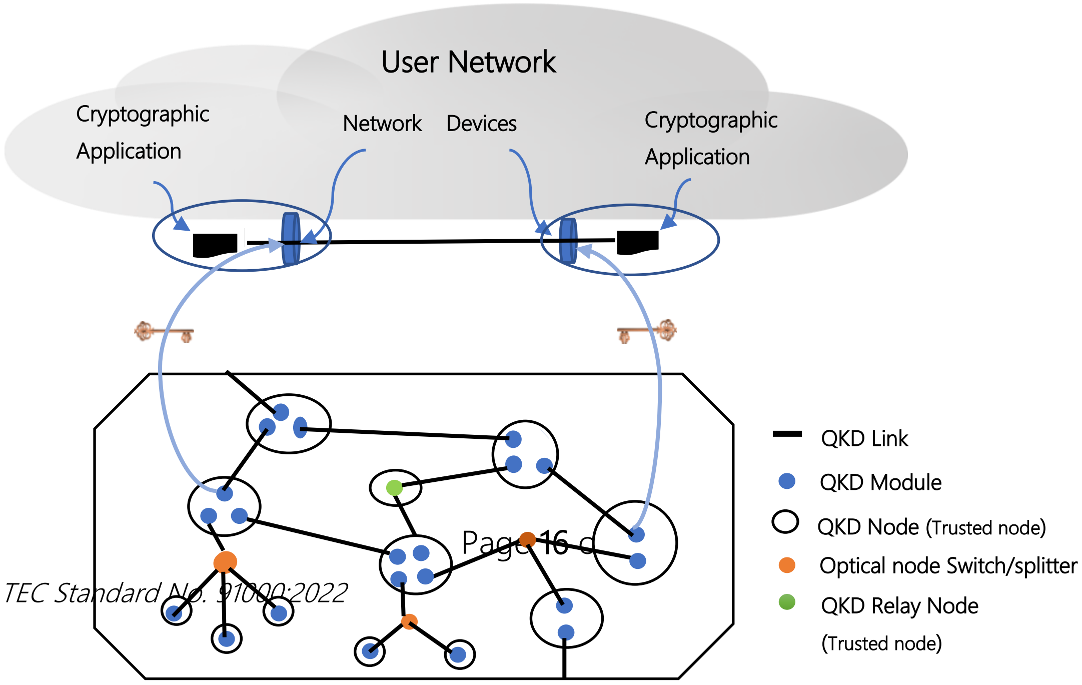
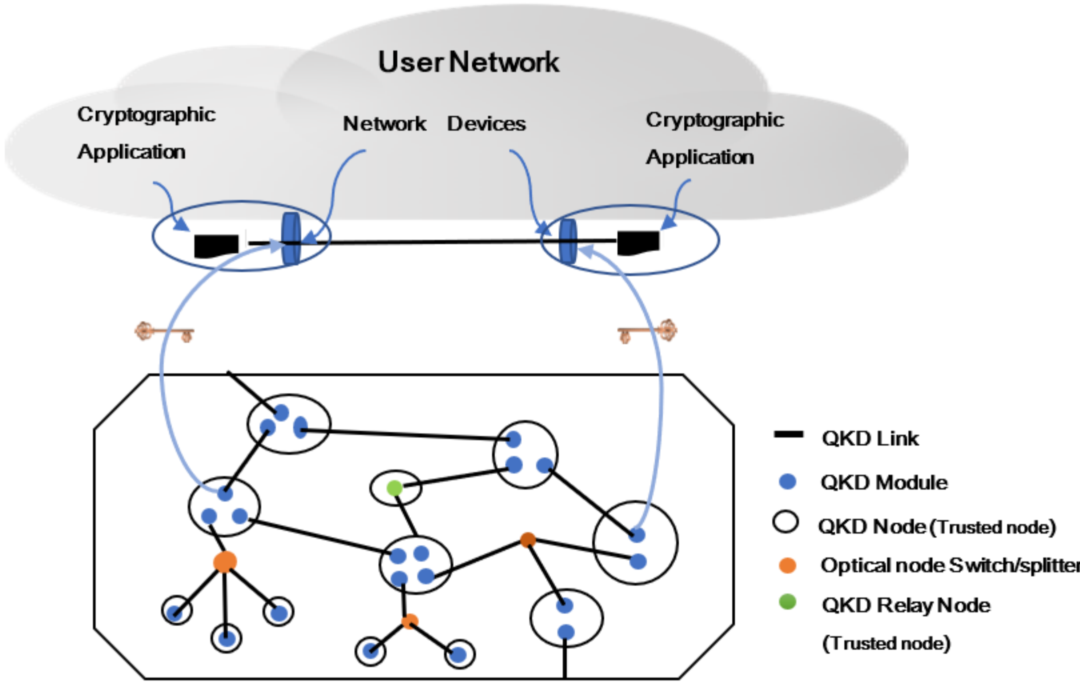


Figure 3C : QKD Ring network topology



~~*Figure 3 Multipoint QKD System*~~

1.1.6 In a multipoint QKD deployment (Figure ~~3~~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 3, 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 3 also illustrates the option of using optical switching/splitting for interconnecting one QKD node with more than one QKD node in a time-shared 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 3 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.


User Network
Cryptographic Application
Network Devices
Cryptographic Application
QKD Link
QKD Module
QKD Node (Trusted node)
Optical node Switch/splitter
QKD Relay Node (Trusted node)

~~1.1.5~~

Figure ~~3~~4 Multipoint QKD System

~~1.1.6 The general characteristics and architecture of QKD Networks shall be compliant with ITU-T Y.3800-3804 as specified in the GR.~~

1.1.7 The GR outlines the general characteristics of QKD systems including technical requirements for P2P and Multipoint QKD Systems.

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.

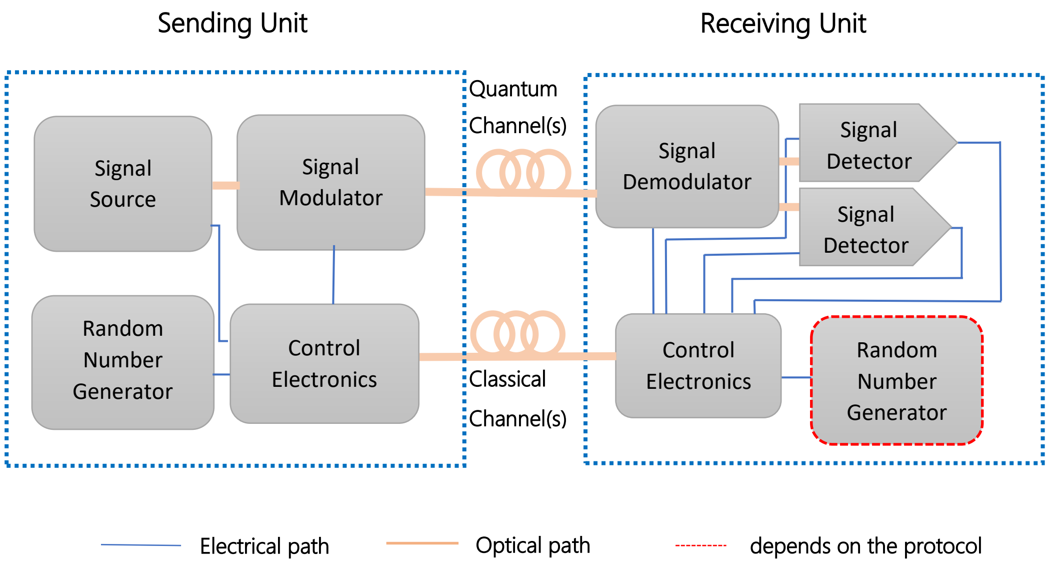


Figure 4-5 QKD System Architecture

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. As of now, these signals are transmitted through classical channels on separate fibre(s) or channel(s). However, there should not be any dependency between the fibres/channels.

1.3 QKD System Description

1.3.1 QKD System Shall provide the following functionalities

a) Interface from/to user/application interface.

b) Key sifting, error estimation/correction and privacy amplification.

c) Key management.

d) Performance monitoring, system configuration and administration, auto-calibration, system health parameters, etc

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) must be ~~below~~ <<1 and mentioned in the product datasheet.~~.~~

1.4.2 Receiver Node

The Receiver's unit shall be a 19" rack-mountable with a height of size 1U/2U/3U, etc. It shall 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.

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.

1.5.3 QKD system shall have provision for changing the mean photon number value using an inbuilt Variable Optical Attenuator (VOA).

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 countermeasures against known experimentally demonstrable quantum/classical channel attacks as provided in Test Schedule and Test Procedure (TSTP).

1.5.5 QKD system shall have provision for changing disclose rate.

1.5.6 QKD system shall have provision for changing privacy amplification rate.

1.5.7 QKD system may have provision for changing information reconciliation algorithm. QKD system shall have provision for changing code rate for Information reconciliation algorithm subjected to secured key remaining tamper proof.

1.5.8 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.

1.5.9 QKD System shall provide the provision for Discrete Variable (DV) Quantum Key distribution protocol/differential phase reference protocols i.e., Coherent One Way (COW), Differential Phase Shift (DPS), etc.

1.5.10 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.

1.5.11 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.

1.5.12 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). 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.

1.5.13 The fibre-media as stipulated in this document shall be compliant with ITU-T G.652D and ITU-T G.655 NZ-DSF and ITU-T G.657 recommendations on single mode optical fibre.

1.5.14 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.

~~1.5.15 The measurement accuracy of input/output power of the Classical Channel(s) (together or separate channels) from the Quantum Key Distribution Network (QKDN) Manager of the system shall be within NIST standards from the actual measured value on a wide-band Optical Power Meter.~~

1.5.15 QKD Modules authentication must be done by a classical channel existing between QKD Modules.

1.5.16 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~~.~~

1.5.17 The QKD Modules must 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.

1.5.18 Secret Key must be generated by each QKD module, Both QKD modules must 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 eg.~~ or~~ Secure Key Integration Protocol (SKIP), etc. as per the requirements of the purchaser~~.~~ ~~European Telecommunications Standards Institute (ETSI) defined standard Interface must be used for the transfer of the secret Key~~.

~~1.5.18~~1.5.19 The QKD module shall provide status information for the module and the associated QKD link through a secure management interface.~~The QKD module must provide status information of the QKD module and optionally of the QKD link. to the Key Manager within the QKD system.~~

~~1.5.19~~1.5.20 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 EVE dropper for necessary corrective action.

~~1.5.20~~1.5.21 The Key Manager must 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.

~~1.5.21~~1.5.22 The Key Manager must 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.

~~1.5.22~~1.5.23 Once Keys are provided by Key Manager to the user network:

(1) The Key Manager must receive key requests from authorized cryptographic applications through the key supply interface.

(2) The Key Manager must supply the requested number of keys to a cryptographic application in the service layer of the user network through the key supply interface.

(3) The Key Manager must supply keys to cryptographic applications in the service layer of the user network through the key supply interface with security capabilities.

1.5.24 The Quantum Key Distribution Transmitter and Quantum Key Distribution Receiver shall support tamper-evident enclosure and secure tamper-event logging.

Technical Requirements for Star Topology:

1.5.25 The Bob node shall function as the central coordinating node, with multiple Alice nodes connected in a star topology.

1.5.26 The Hub shall include an optical switch as a stand-alone unit or integrated into QKD module to support optical switching.

1.5.27 The system shall support automatic optical switching between different connected Alice nodes without any manual intervention.

1.5.28 The switching time between connected nodes shall be user-configurable.

~~Switching between connected nodes shall not require recalibration of the system after an initial one-time calibration for each node.~~

1.5.29 The system shall support the connection ~~of up to 8~~atleast 2 Alice nodes to the central coordinating node.

1.5.30 The Hub (Bob) shall act as key relay to establish a secure connection using QKD keys between Alice nodes.

1.5.31 All the nodes shall provide QKD secure Keys to the cryptographic applications using standard ETSI GS QKD 014.

1.6 Performance Requirement of QKD System

1.6.1 Online Performance Monitoring

The QKD modules must 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 must monitor and report optical layer performance in real time to Local Craft Terminal (LCT)/ Element Management System (EMS).

The system shall support the following measurements:

a. Quantum Bit Error Rate (QBER)

b. Key Rate

c. Visibility (~~as applicable to a protocol~~applicable for COW protocol)

d. Mean Photon Number

e. SPD parameters like dead time, efficiency, etc.

f. Quantum channel transmit ~~and receive~~ power

g. On-demand ~~offline~~ randomness ~~Real-time monitoring of randomness on-demand~~

h. Key symmetry

1.6.2 QBER performance shall be less than 5% (desirable) for the Quantum Channel Loss specified in table 1. Higher QBER is acceptable for higher Quantum Channel loss and the equipment vendor needs to provide the corresponding values before offering the equipment for TEC Certification.

1.6.3 Visibility performance (f~~F~~or COW QKD) over a simulated section shall be tested for 24 hours and visibility performance shall be better than 90%.

1.7 Technical Specifications of QKD System

1.7.1 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.

1.7.2 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~~ or Secure Key Integration Protocol (SKIP)~~.

Table 1: Specifications:

S.No.	Specification Description	Value			
1.	Secure Key Rate	>2Kbps for DPS protocol			
		>1Kbps for COW protocol			
2.	QBER	<5%			
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 differential phase reference protocols	Type of the product	Short Range	Long Range	Extended Range
		Application	<50 km	50-80 km	>80 km
		Channel Loss (maximum)	12dB	18dB	23dB
8.	Operating Temperature	10 to 25 °C			
9.	Detector Type	SPD (SPAD / SNSPD /etc)			
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	Over Classical Channel

1.8 Technical Requirements of Multipoint QKD System

1.8.1 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.

1.8.2 A Multipoint QKD system shall include:

- **Key Manager:** To receive and manage keys generated by QKD modules and QKD links, relay the keys, and supply the keys to cryptographic applications.
- **QKDN Controller:** To control QKDN resources to ensure secure, stable, efficient, and robust operations of a QKDN.
- **QKDN Manager:** To manage fault, configuration, accounting, performance and security (FCAPS) aspects of a QKDN as a whole, and support user network management.

~~1.8.1~~ Technical Requirements of Key Manager:

~~1.8.2 A QKD link may include one or more quantum relay points to extend QKD distance. Different QKD links may use different QKD protocols.~~

1.8.3 ~~The~~ The Key Manager shall receive keys from a QKD module(s) via an appropriate interface, and store them securely.

1.8.4

1.8.5 ~~QKD module must provide status information of the QKD module and optionally of the QKD link to the QKDN controller.~~ The Key Manager may perform the following tasks: Key re-size, key re-format (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.

1.8.6 The Key Manager shall be compatible with various kinds of QKD modules which implement different protocols.

~~1.8.4~~ The Key Manager shall receive status information of QKD module(s) and QKD link(s) from the QKD module(s) in the quantum layer.

1.8.7

~~1.8.5~~1.8.8 The Key Manager (KM) ~~must~~ 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.

~~1.8.6~~1.8.9 The Key Manager ~~must~~ shall provide fault and performance information of the Key Manager and Key Manager links to the QKDN manager.~~.~~

~~1.8.7~~1.8.10 The Key Management unit must include secure hardware ~~called Secure System~~ 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.

~~1.8.8 The Key Manager may perform the following tasks: Key re-size, key re-format (necessary headers and footers such as key ID, generation date, key length, etc., for key management), key storage; acquisition of QKD link parameters which may include QBER, key rate, link status, etc. The Key Manager is optionally recommended to format keys where necessary for internal purposes or for key supply or key relay, including combining or splitting where lengths are not appropriate.~~

~~1.8.9~~1.8.11 The Key Manager ~~is optionally recommended to~~shall support key relay~~s for~~ employing highly secure encryption (eg; one-time pad (~~like~~ OTP)) ~~through~~ 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).

~~1.8.10~~1.8.12 The Key Manager ~~and KM links are~~is o~~O~~ptionally recommended to have capabilities of key synchronization, entity authentication and message authentication to make Key Relaying reliable and secure.

~~1.8.11~~1.8.13 The Key Managers ~~are~~ is optionally recommended to cooperate with each other under the control of the QKDN controller to make key relay efficient.~~.~~

1.8.14 The Key Manager is optionally recommended to 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 is optionally recommended to support access control of cryptographic applications.

1.8.15 The Key Manager shall present a key supply interface that various cryptographic applications can utilize to send key requests.

1.8.16 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.

1.8.17 The Key Manager shall supply keys to cryptographic applications via a key supply interface with security capabilities.

1.8.18 The Key Manager shall support access control of cryptographic applications.

1.8.19 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.).

~~1.8.12~~ Technical Requirements of QKDN Controller:

~~1.8.13~~1.8.20 The QKDN controller must control key relay routes including rerouting between the two endpoints of cryptographic applications which require the key. ~~Key relay control may be based on a request from the service layer.~~

~~1.8.14~~1.8.21 The QKDN controller must control the status of the key management layer and quantum layer.

~~1.8.15~~1.8.22 The QKDN controller ~~must~~ shall control the reconfiguration of the QKD link if failure or eavesdropping occurs.

~~1.8.16~~1.8.23 The QKDN controller ~~must~~ shall provide fault, performance, accounting, and configuration information to a QKDN manager.

1.8.24 The QKDN controller ~~must~~ 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.

1.8.25 The QKDN controller is optionally recommended to provide charging policy control.

1.8.26 The QKDN controller is optionally recommended to 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.

1.8.27 The QKDN controller is optionally recommended to provide quality of service (QoS) policy control.

~~1.8.17~~ The QKDN controller is optionally recommended to support and ensure access control of functional elements in the quantum layer and the key management layer.

1.8.28

Technical Requirements of QKDN Manager:

~~1.8.18~~

1.8.29 The QKDN manager must support fault management, accounting management, configuration management, performance management and security management.

1.8.30 The QKDN manager shall provide fault management to support:

- collecting/receiving status information provided by the quantum, key management, and QKDN control layers;
- analysing the status information collected/received for fault indicators.

~~1.8.19~~

1.8.31 The QKDN manager is required to provision and configure~~s~~ the managed resources in each layer.

~~1.8.20~~1.8.32 The QKDN manager is required to support routing and rerouting of key relay.

~~1.8.21~~1.8.33 The QKDN manager is optionally recommended to ~~manage the network topology of each layer.~~support management of the network topology.

~~1.8.22~~1.8.34 The QKDN manager is optionally recommended to perform inventory management for all the QKDN resources in each layer.

~~1.8.23~~1.8.35 The QKDN manager is optionally recommended to manage the life cycle of the resource repositories (e.g., create, store, retrieve, modify, remove, etc.) in each layer.

~~1.8.24~~1.8.36 The QKDN manager must monitor QKD link failures to support QKD modules for appropriate recovery actions including reconfiguration of QKD links and rerouting of key relay routes.

~~1.8.25~~1.8.37 The QKDN manager is optionally recommended to provide fault detection and root-cause analysis/diagnosis capability for quantum, key management, and QKDN control layers.

~~1.8.26~~1.8.38 The QKDN manager is optionally recommended to make decisions and generation failure resolving policies and interacts with each layer for correction of faults.

~~1.8.27~~1.8.39 The QKDN manager is optionally recommended to discover each layer managed resources and functions and bootstrap to make them ready for the operation based on the bootstrapping policies.

~~1.8.281.7.1 The QKDN controller is optionally recommended to provide charging policy control.~~

~~1.8.291.7.1 The QKDN controller is optionally recommended to provide session control.~~

~~1.8.301.7.1 The QKDN controller is optionally recommended to provide quality of service (QoS) policy control.~~

~~1.8.311.7.1 The QKDN controller is optionally recommended to support and ensure access control of functional elements in the quantum layer and the key management layer.~~

~~1.8.32~~1.8.40 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.

~~1.8.33~~1.8.41 The QKDN manager must collect the performance data and status of each layer, register them into a performance database and updates them.

~~1.8.34~~1.8.42 The QKDN manager must analyse the performance of collected data and generate~~s~~ performance reports (Performance Management).

~~1.8.35~~1.8.43 The QKDN manager must manage the key supply service policies (Performance Management).

~~1.8.36~~1.8.44 The QKDN manager must collect management information including event logs, audit trails, and so on from each layer for detecting security anomalies.

~~1.8.37~~1.8.45 The QKDN manager must support key life cycle management by KMs, ensuring traceability of keys by using the log database.

~~1.8.38~~1.8.46 The QKDN manager is optionally recommended to 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.

~~1.8.39~~1.8.47 The QKDN manager is optionally recommended to manage the key management policies and transmits them to the QKDN controller.

~~1.8.40~~1.8.48 The QKDN manager is optionally recommended to perform cross-layer management orchestration and also to support management requests from a user network management.

~~1.8.41~~1.8.49 The QKDN manager must monitor the status of the whole QKDN.

~~1.8.42~~1.8.50 The QKDN manager must authenticate and authorize management. For example, management of the identification and registration of modules in a QKDN, and their access rights.

~~1.8.43~~1.8.51 The QKDN manager is optionally recommended to provide QoS management and charging management.

~~1.8.44~~1.8.52 The QKDN manager must detect eavesdropping attempts against a quantum channel.

~~1.8.45~~1.8.53 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.

~~1.8.46~~1.8.54 The QKDN manager must support the QKDN controller for routing and rerouting of key relays including instruction of policies and rules caused by the faults or performance degradation.

~~1.8.47 The QKDN must support the QKDN controller for provisioning of routing and re-routing of key relay routes if QKDN supports key relay as the configuration management function.~~

~~1.8.48 The QKDN shall have a unique identifier for its classical and quantum channels 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.~~

~~1.8.49~~1.8.55 The QKDN manager may optionally provide the QKDN resource provisioning requested by the user network manager.

1.8.56 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.).

1.8.57 QKDN manager shall provide a graphical user interface (GUI) for network monitoring and management.

1.8.58 QKDN manager shall support Multi-Factor Authentication (MFA) for all administrative and privileged user access.

1.8.59 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.

1.8.60 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.

~~1.8.50~~1.8.61 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.

~~1.8.51 The QKDN may optionally have the capability to co-operate with the user network either in an integrated or independent management manner.~~

1.8.62 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.

1.8.63 The QKDN must record all configuration changes, policy updates, and operator actions in an auditable change-history store.

~~1.8.52~~1.8.64 The QKDN must have network control and management capabilities.

~~1.8.53~~1.8.65 The QKDN must 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.

~~1.8.54~~1.8.66 The QKDN must have the capability to use optical fibre channels or direct free space optical channels for quantum channel networking.

~~1.8.55~~1.8.67 The QKDN must be capable of automatically authenticating and operating QKD nodes that are rebooted.

1.8.68 The QKDN may have the capability to manage QoS by taking into account the request from the user network.

1.8.69 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.

1.8.70 The communication interface between the QKD Module, QKDN controller and the QKDN manager shall be secured, using Classical or Post Quantum Cryptographic Algorithms.

1.8.71 QKDN manager and QKDN controller may optionally support a High Availability (HA) deployment. This architecture must ensure continuous operation of the QKDN manager and QKDN controller. This can be achieved through either of these options:

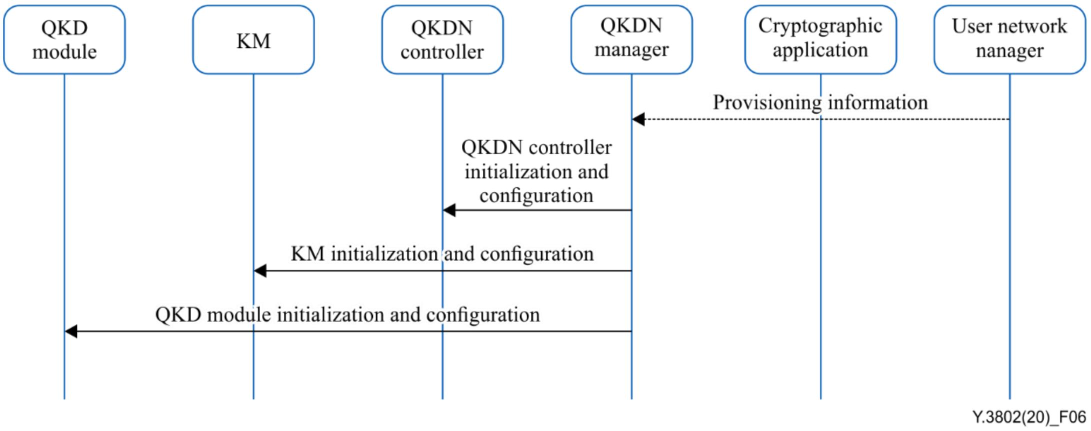
- Active-Standby: An active primary instance is backed up by a redundant standby instance, ready to take over in case of a failure.
- ~~1.8.56~~ Active-Active: Multiple instances run simultaneously, sharing the workload and providing instant failover.

~~1.8.57~~1.8.72 The equipment ~~must~~ may support Dual stack IP addresses (IPv4 & IPv6) for management and services.

1.9 Operational Procedures for the QKDN:

1.9.1 Service provisioning and system initialization procedure

The below figure illustrates a procedure for service provisioning and system initialization for a multi-point QKD system.



QKD module
KM
QKDN controller
QKDN manager
Cryptographic application
User network nanager
Provisioning information
QKDN controller initialization and configuration
KM initialization and configuration
QKD module initialization and configuration
Y.3802(20)_F06

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.

- 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.
- 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.

1.9.2 Key generation procedure:

The below figure illustrates a procedure for key generation in multi-point QKD system.

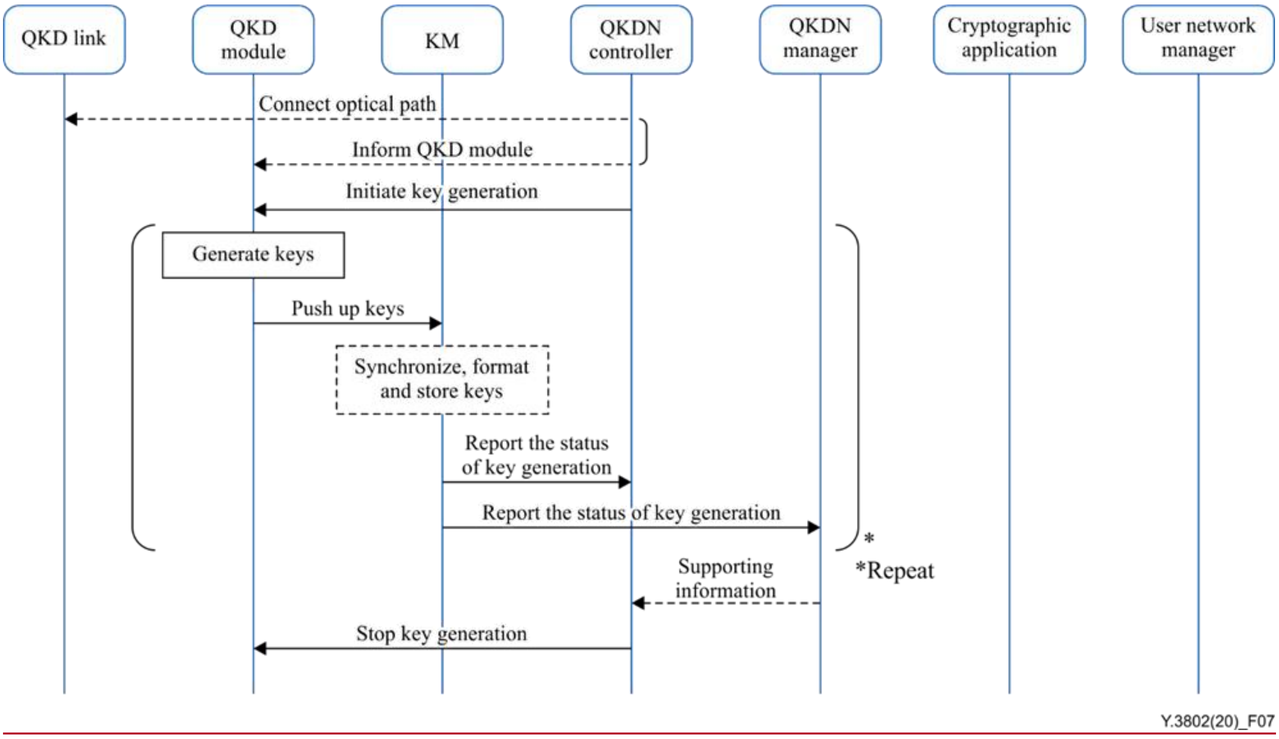


Figure 7 Key generation procedure

1. 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.
2. 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.
3. The QKD modules send and/or receive quantum signals and then perform synchronization of quantum signals and key distillation for key generation.
4. The QKD modules push up the generated keys to KMs.
5. The KMs optionally synchronize, format and store these keys if necessary.

6. The KMs report the status of key generation to the QKDN controller and the QKDN manager for control and management functions respectively.

7. The sequence from step 3 to step 6 can be repeated (and often executed in parallel) until a sufficient number of keys are generated.

8. The QKDN manager optionally sends supporting information to the QKDN controller if necessary.

9. 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.

1.9.3 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

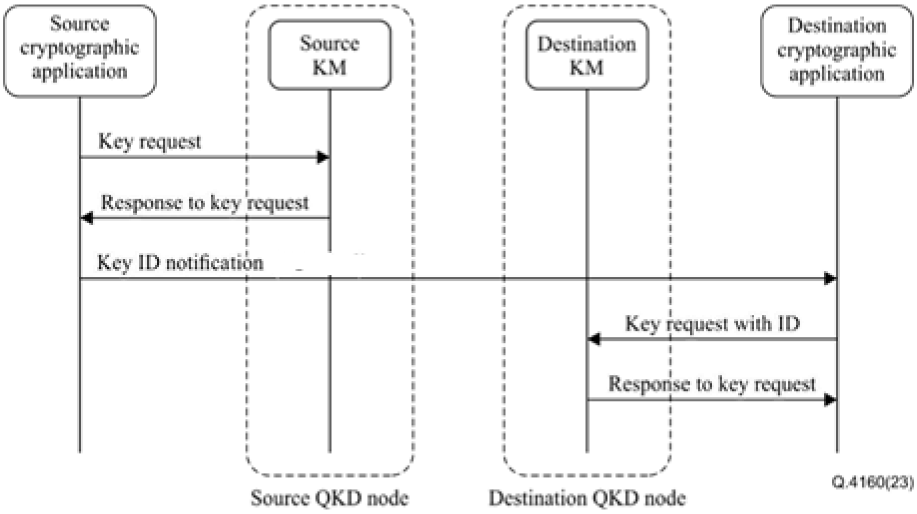


Figure 8 Signalling procedures for key supply upon request mode implemented by two QKD nodes

1. The source cryptographic application sends a "key request" message to the source KM at the source QKD node.
2. The source KM responds "response to key request" message to the source cryptographic application with the keys requested and the corresponding key IDs.

3. The source cryptographic application sends a "key ID notification" message to the destination cryptographic application with the key IDs.
4. 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.
5. The destination KM responds "response to key request" message to the destination cryptographic application with the keys requested.

1.9.4 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.

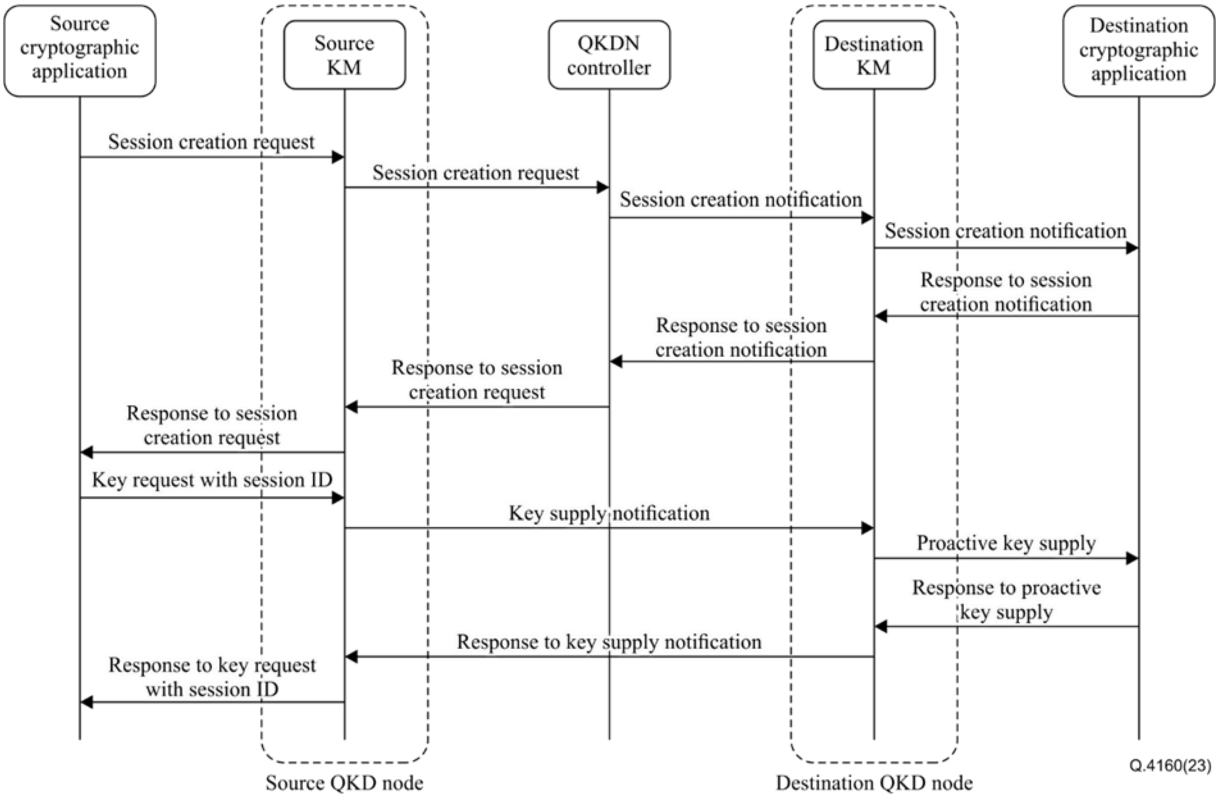

Source cryptographic application
Source KM
QKDN controller
Destination KM
Destination cryptographic application
Session creation request
Session creation request
Session creation notification
Session creation notification
Response to session creation notification
Response to session creation notification
Response to session creation request
Response to session creation request
Key request with session ID
Key supply notification
Proactive key supply
Response to proactive key supply
Response to key supply notification
Response to key request with session ID
Source QKD node
Destination QKD node
Q.4160(23)

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

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

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

3. 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.

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

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

6. 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.

7. 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.

8. The source KM responds "response to session creation request" message to the source cryptographic application with the received session ID.

9. 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.

10. 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.

11. The destination KM sends a "proactive key supply" message to the destination cryptographic application with the notified number of keys.

12. The destination cryptographic application responds "response to proactive key supply" message to the destination KM with the key IDs of the received keys.

13. The destination KM responds "response to key supply notification" message to the source KM with the received key IDs.

14. 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.

1.9.5 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.

1. 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.
2. 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.

3. The KM2 in QKD node 2 performs a key relay to the KM3 in the QKD node 3 according to the key relay route.

4. 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.

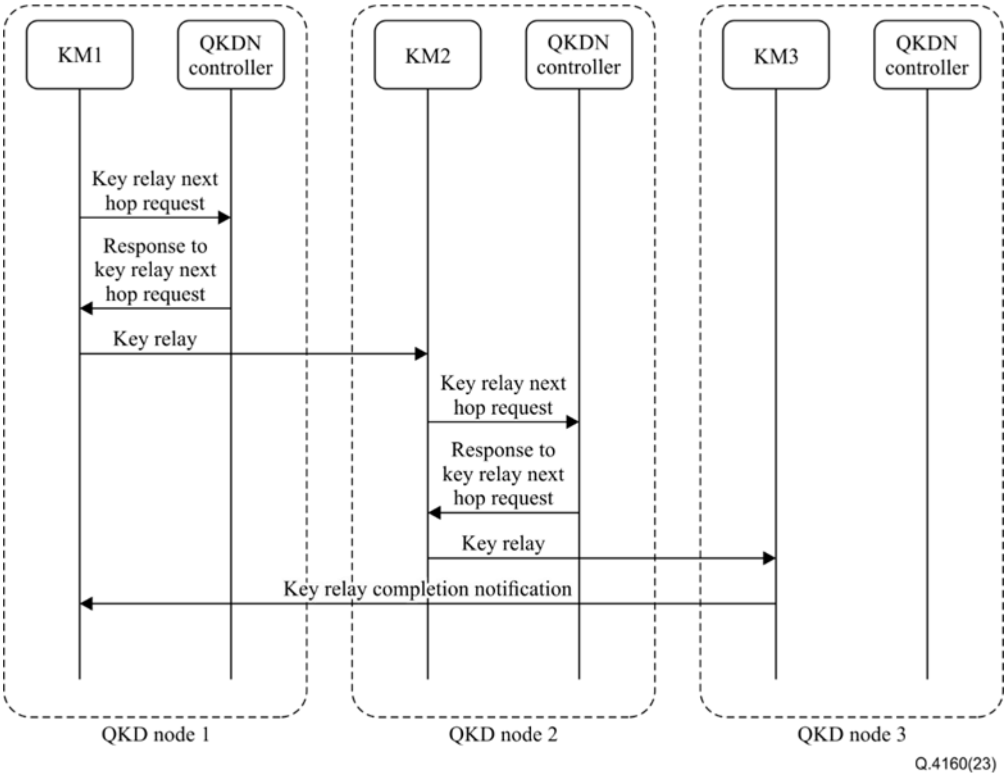

KM1
QKDN controller
KM2
QKDN controller
KM3
QKDN controller
Key relay next hop request
Response to key relay next hop request
Key relay
Key relay next hop request
Response to key relay next hop request
Key relay
Key relay completion notification
QKD node 1
QKD node 2
QKD node 3
Q.4160(23)

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

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

1. 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".

2. 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.

3. 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.

4. 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.

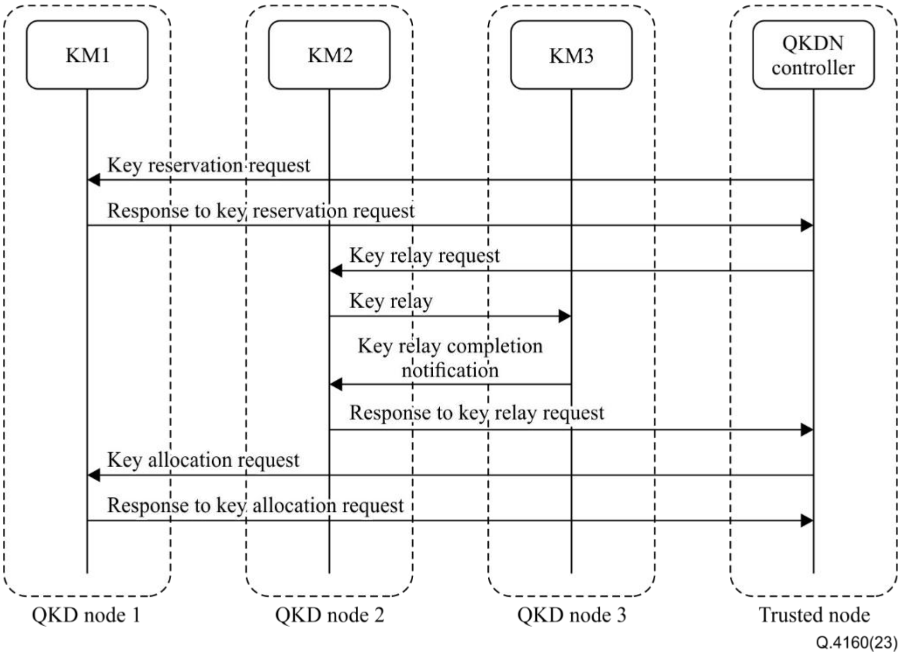


Figure 10B Typical signalling procedures for key relay for a centralized QKDN with key reservation

1.9.6 Key request, key relay, and key supply

A. Distributed QKDN:

The below figure shows typical signalling procedures for key request, key relay, and key supply for a distributed QKDN:

1. 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.
2. 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.

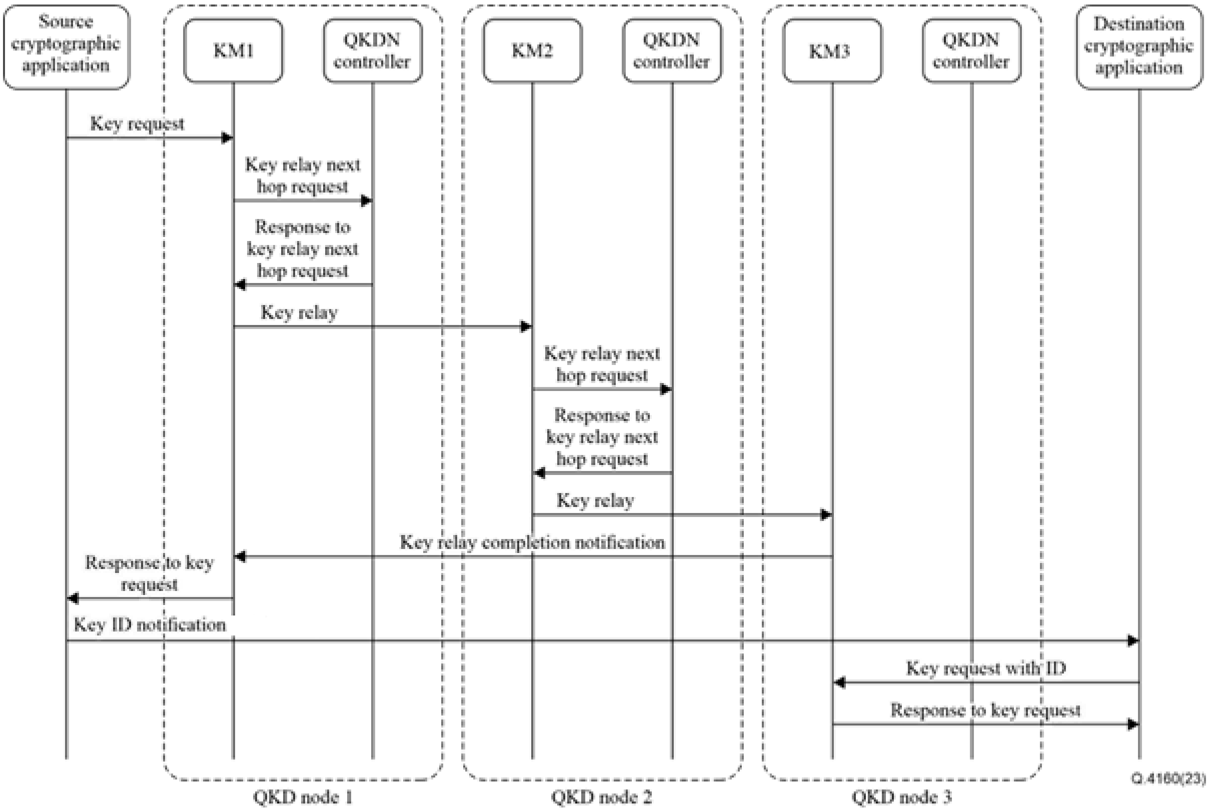

Source cryptographic application
KM1
QKDN controller
KM2
QKDN controller
KM3
QKDN controller
Destination cryptographic application
Key request
Key relay next hop request
Response to key relay next hop request
Key relay
Key relay next hop request
Response to key relay next hop request
Key relay
Key relay completion notification
Response to key request
Key ID notification
Key request with ID
Response to key request
QKD node 1
QKD node 2
QKD node 3
Q.4160(23)

Figure 11A Typical signalling procedures for key request, key relay, and key supply for distributed QKDNs

3. The KM2 and the QKDN controller in the QKD node 2 performs the same procedures as the KM1 of the QKD node 1.
4. 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.

5. The source cryptographic application sends a "key ID notification" message to the destination cryptographic application with a key ID.
6. 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).
7. The nearest KM (shown as KM3 in the figure) responds "response to key request" message with keys to the destination cryptographic application.

B. Centralized QKDN:

The figure shows typical signalling procedures for key request, key relay, and key supply for a centralized QKDN.

1. 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.
2. 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.

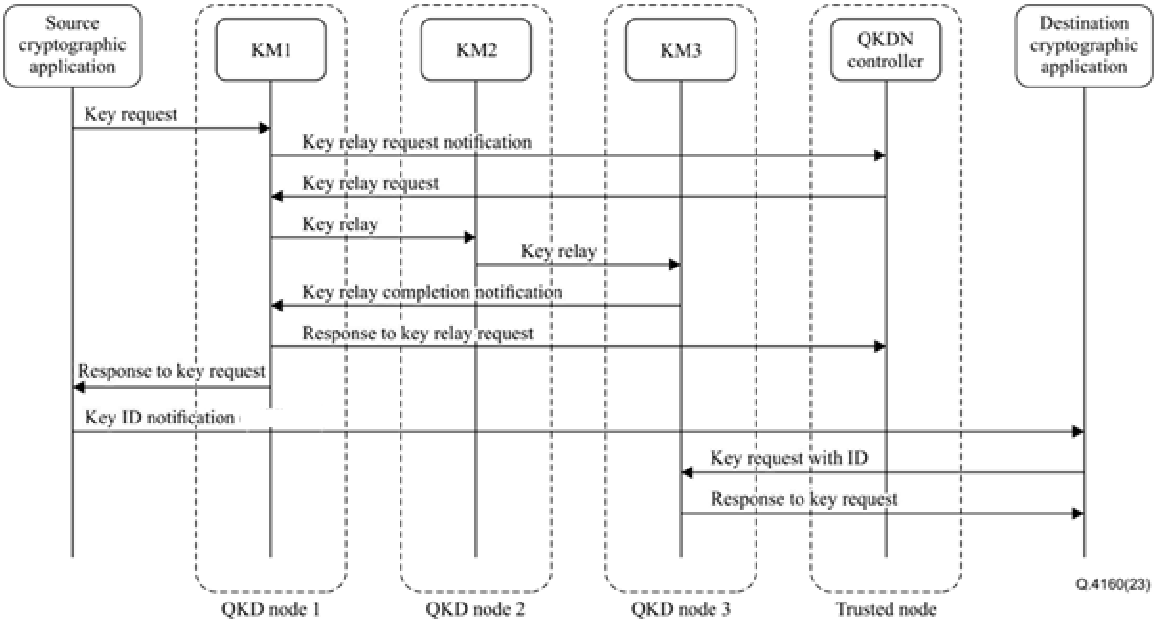


Figure 11B – Typical signalling procedures for key request, key relay, and key supply for centralized QKDNs

~~1.~~3. 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.

4. 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.

5. The source cryptographic application sends "key ID notification" message to the destination cryptographic application with the key ID.

~~2.~~6. 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).

~~3.~~7. 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.

2.1.2 Relevant ITU-T Recommendations & other specifications are given in the GR.

2.1.3 All references to TEC GRs & other Recommendations imply their latest issues.

2.2 Engineering requirements

2.2.1 The manufacturers shall furnish the actual 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.

2.2.3 The system shall work in an environment with 10°C to 25°C temperature and 80% Rh.

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.

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.

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.

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.

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.

2.2.10 Important Do's and Don'ts about the operation of the system shall be indicated.

2.3 Operational requirements

2.3.1 The equipment shall be designed for continuous operation.

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.

2.3.3 Visual indication to show power ON/OFF status shall be provided.

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.

2.4 Quality requirements

2.4.1 ~~The manufacturer shall furnish the Mean Time Between Failures (MTBF)/ Mean Time to Repair (MTTR) values. The calculations shall be based on the guidelines as in the Bharat Sanchar Nigam Limited (BSNL)- Quality assurance (QA) document: QM-115 - "Reliability Methods and Predictions" or any other international standard.~~The manufacturer shall furnish the MTBF value along with the methodology used for calculation. The minimum value of MTBF shall be 25,000 hrs.~~.~~

2.4.2 The equipment shall be manufactured in accordance with the international quality management system ISO 9001:2015 or latest issue~~for which the manufacturer should be duly accredited~~. A quality plan describing the quality assurance system followed by the manufacturer would be required to be submitted by the manufacturer.

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.

2.5.2 The equipment shall have easy access for servicing and maintenance.

2.5.3 Suitable alarms shall be provided for the identification of faults in the system and faulty units.

2.5.4 Ratings and types of fuses used are to be indicated by the supplier.

2.6 Power supply requirements for QKD Equipment

2.6.1 The QKD system may be provided with two power feeds.

a) centralized power supply with 1+1 redundancy and

b) Distributed onboard power supply.

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.

2.6.3 The equipment shall operate over this range without any degradation in performance.

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.

2.6.5 The derived DC voltages in the equipment shall have protection against over-voltage, short-circuit and overload.

2.6.6 The equipment shall be power efficient. ~~The power consumption shall be minimal.~~ The actual power rating/ consumption is to be furnished by the manufacturer of the equipment.

2.7 Accessories

2.7.1 The supplier shall provide a complete set of:

a) ~~a)~~ 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.

b) Software, along with software version and the arrangement to load the software at site.

2.8 Documentation

Technical literature in the English language only shall be accepted.

2.7.2 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.

2.7.3 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.

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.

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.

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.

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 must be mentioned in the QKD equipment. An undertaking/test certificate shall be sufficient during certification.

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.

2.10.5 The equipment shall have a terminal for grounding the rack.

2.10.6 All switches/controls on the front panel shall have suitable safeguards against accidental operation.

2.10.7 The equipment shall be adequately covered to safeguard against entry of even dust, insects, etc.

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:

(1) P2P QKD system without Trusted Relay node

(2) P2P QKD system with Trusted Relay node

(3) ~~P2P~~ QKD system with Star Topology

~~(4) P2P QKD system with Ring Topology~~

(~~5~~4~~3~~) Multipoint QKD system

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 ~~or Point to Multipoint QKD System) filed~~ 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.

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;

Table 2: Environmental Testing Requirement

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

		days: 25 °C Ambient Temp: 20°C	
4	Rapid Temperature Cycling Test	LST: 10 °C HST: 25°C. Ambient Temp: 20°C	NA
5	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 - Part 1: Safety requirements"~~Electrical safety: IEC 62368-1 [replaced IS 13252-1/IEC 60950-1] is a basic reference for the safety of telecommunications equipment. In all cases, active electronics must comply with locally applicable electrical safety requirements. This may include electrical insulation, grounding, fuses, current loss switches, etc. In case remote line powering is applied, it should comply with [ITU-T K.50], [ITU-T K.51] and [IEC 60950-21].~~

~~The safe working practices described in [ITU-T K.64] should be followed when work is carried out on outside plant electronic equipment.~~

3.1.2 Laser safety: Since the box should house active optical devices, it should comply with IEC 60825- 1 and IS 14624-2/IEC 60825-2 for optical safety requirements.

Note: This test shall be applicable if laser components are directly mounted in the box.

~~3.2 Electromagnetic Interference~~

~~The QKD equipment shall conform to the EMC requirements.~~

~~3.3~~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 ~~by~~ from an accredited test agency.

~~3.3.1~~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~~ (2015)~~.

ii. For Radiated Emission tests, limits below 1 GHz shall be for measuring at a distance of 3m.

OR

~~3.3.2~~ **Conducted and radiated emission (applicable to instruments such as power meter, frequency counter, etc.):**

Name of EMC Standard: "~~As per~~ CISPR 11 {2024~~15~~} - Industrial, Scientific and Medical (ISM) radio-frequency equipment - Electromagnetic disturbance characteristics- Limits and methods of measurement" ~~for the following~~

Limits:

i. To comply with the category of Group 1 of Class B of CISPR 11 {2024~~15~~}

ii. The values of limits shall be as per clause No. 8.5.2 of TEC Standard No. ~~TEC/SD/DD/EMC-221/05/OCT-16~~11016:201~~2~~6.

~~3.3.3~~3.2.2 Immunity to Electrostatic discharge:

Name of EMC Standard: ~~As per~~ IEC 61000-4-2 {2008} "Testing and measurement techniques of Electrostatic discharge immunity test"~~ for the following~~

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~~/SD/DD/EMC-221/05/OCT-16~~ 11016:2016.

Applicable Performance Criteria shall be as per Table 3 under Clause 7.2 of TEC Standard No. -TEC 11016:2016~~TEC/SD/DD/EMC-221/05/OCT-16~~.

~~3.3.4~~3.2.3 Immunity to radiated RF:

Name of EMC Standard: ~~As per~~ IEC 61000-4-3 (202~~1~~0) "Testing and measurement techniques-Radiated RF Electromagnetic Field Immunity test" ~~for the following~~

Limits:

(i) For Telecom Equipment and Telecom Terminal Equipment with Voice interface (s)

a. Under test level 2 {Test field strength of 3 V/m} for general purposes in the frequency range 80 MHz to 1000 MHz and

b. 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)

a. 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~~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 11016:2016~~TEC/SD/DD/EMC-221/05/OCT-16~~.

~~3.3.5~~3.2.4 Immunity to fast transients (burst):

Name of EMC Standard: ~~As per~~ IEC 61000- 4- 4 {2012) "Testing and measurement techniques of electrical fast transients / burst immunity test" ~~for the following.~~

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~~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 11016:2016~~TEC/SD/DD/EMC-221/05/OCT-16~~.

~~3.3.6~~3.2.5 Immunity to surges:

Name of EMC Standard: As per IEC 61000-4-5 (2014) "Testing & Measurement techniques for Surge immunity test"~~ for the following.~~

Limits:

(i) For mains power input ports:

(a) 1.0 kV peak open circuit voltage for a line-to-ground coupling.

(b) 0.5 kV peak open circuit voltage for a line-to-line coupling.

(c) 2.0 kV peak open circuit voltage for a line-to-line coupling.

ii) For telecom ports:

(a) 1.0 kV peak open circuit voltage for line to ground.

(b) 0.5 kV peak open circuit voltage for line-to-line coupling.

(c) 2.0 kV peak open circuit voltage for line-to-line coupling.

Performance Criteria shall be as per Table 1 under Clause 6 of TEC Standard No. TEC 11016:2016~~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 11016:2016~~TEC/SD/DD/EMC-221/05/OCT-16~~.

~~3.3.7~~3.2.6 Immunity to conducted disturbance induced by Radio frequency fields:

Name of EMC Standard: ~~As per~~ IEC 61000-4-6 (202~~1~~3) "Testing & measurement techniques-Immunity to conducted disturbances induced by radio- frequency fields" ~~for the following.~~

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.

~~3.3.8~~3.2.7 Immunity to voltage dips & short interruptions (applicable to only ac mains power input ports, if any):

Name of EMC Standard: ~~As per~~ IEC 61000-4-11 (2020~~04~~) "Testing & measurement techniques- voltage dips, short interruptions and voltage variations immunity tests" ~~for the following.~~

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.

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~~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 11016:2016~~TEC/SD/DD/EMC-221/05/OCT-16~~.

~~3.3.9~~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.

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)~~TEC/SD/DD/EMC-221/05/OCT-16~~ 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). ~~(a) to (g).~~ The details of IEC/CISPR and their corresponding Euro Norms are as follows:

IEC/CISPR	Euro Norm
CISPR 11	EN 55011
CISPR 22	EN 55022
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

DEFINITIONS, ACRONYMS AND TERMINOLOGY

Application link: A communication link used to provide cryptographic applications in the user network.

Classical channel: A Communication channel: that is used by two communicating parties for exchanging data encoded in a form that may be non-destructively read and fully reproduced.

Disclose rate: It is the percentage of detection event values shared by the Receiver with the Sender estimated by the Quantum Bit Error Rate (QBER).

Information theoretically secure (IT-secure): Secure against any deciphering attack with unbounded computational resources.

Key life cycle: A sequence of steps that a key undergoes from its reception by a key manager (KM) through its use in a cryptographic application and until deletion or preservation depending on the key management policy.

Key management: All activities performed on keys during their life cycle starting from their reception from the quantum layer, storage, formatting, relay, synchronization, authentication, to supply to a cryptographic application and deletion or preservation depending on the key management policy.

Key manager (KM): A functional module located in a quantum key distribution (QKD) node to perform key management in the key management layer.

Key manager link: A communication link connecting key managers (KMs) to perform key management.

Key relay: A method to share keys between arbitrary quantum key distribution (QKD) nodes via intermediate QKD node(s).

Key supply: A function providing keys to cryptographic applications.

Key symmetry: Here the key symmetry means that the probability detection of bit ‘0’ and bit ‘1’ should be near to equal. NIST randomness test has to be performed on the raw key (bits detected by SPD) to validate the symmetry.

Quantum channel: Communication channel for transmitting quantum signals.

Quantum key distribution (QKD): Procedure or method for generating and distributing symmetrical cryptographic keys with information theoretical security based on quantum information theory.

Quantum key distribution module: A set of hardware and software components that implements cryptographic functions and quantum optical processes, including quantum key distribution (QKD) protocols, synchronization and distillation for key generation and is contained within a defined cryptographic boundary.

Quantum key distribution network (QKDN): A network comprised of two or more quantum key distribution (QKD) nodes connected through QKD links.

Quantum key distribution network controller: A functional module, which is located in a quantum key distribution (QKD) network control layer to control a QKD network.

Quantum key distribution link: A communication link between two quantum key distribution (QKD) modules to operate the QKD.

Quantum key distribution node: A node that contains one or more quantum key distribution (QKD) modules protected against intrusion and attacks by unauthorized parties.

Quantum key distribution network manager: A functional module, which is located in a quantum key distribution (QKD) network management layer to monitor and manage a QKD network.

Quality of service (QoS): The collective effect of service performances, which determines the degree of satisfaction of a user of a service. It is characterized by the combined aspects of performance factors applicable to all services, such as service operability performance; service accessibility performance; service retainability performance; service integrity performance; and other factors specific to each service.

Sender/ Receiver: This document defines the sender/transmitter as Alice and the receiver as Bob.

User network: A network in which cryptographic applications consume keys supplied by a quantum key distribution (QKD) network.

ABBREVIATIONS

For the purpose of this document the following abbreviations apply:

AC	Alternating Current
ALSD	Automatic Laser Shut Down
APR	Automatic Power Reduction
API	Application Programming Interface
BSNL	Bharat Sanchar Nigam Limited
CISPR	International Special Committee on Radio Interference
COW	Coherent One Way
CV	Continuous Variable
DC	Direct Current
DoT	Department of Telecommunications
DPS	Differential Phase Shift
DRBG	Deterministic Random Bit Generator
DV	Discrete Variable
EMC	Electro Magnetic Compatibility
EMS	Element Management System
ETSI	European Telecommunications Standards Institute
FC	Ferrule Connector
GR	Generic Requirements
ID	Identity
IEC	International Electrotechnical Commission
IP	Internet Protocol
IR	Interface Requirements
IS	Indian Standard
ISM	Industrial, Scientific and Medical
ISO	International Organisation for Standardisation
IT	Information Technology
ITU	International Telecommunication Union
KM	Key Manager
LC	Lucent Connector

LCT	Local Craft Terminal
MTBF	Mean time between failures
MTTR	Mean time to repair
NIST	National Institute of Standards and Technology
NZ-DSF	Non-zero dispersion-shifted fiber
PRNG	Pseudo Random Number Generator
P2P	Point-to-Point
PQC	Post-Quantum Cryptography
QA	Quality assurance
QBER	Quantum Bit Error Rate
QKD	Quantum Key Distribution
QKDN	Quantum Key Distribution Network
QKD-Rx	QKD Receiver (Bob)
QKD-Tx	QKD Transmitter (Alice)
QM	Quality Management
QRNG	Quantum Random Number Generator
RTECs	Regional Telecom Engineering Centers
SC	Subscriber Connector
SNSPD	Superconducting Nanowire Single Photon Detector
SPAD	Single Photon Avalanche Photo Detector
SPD	Single Photon Detector
SR	Service Requirements
ST	Straight Tip
TEC	Telecommunication Engineering Centre
TRNG	True Random Number Generator
TSTP	Test Schedule and Test Procedure
VOA	Variable Optical Attenuator
WDM	Wavelength Division Multiplexing

----End of the document----