प्रारूप टेस्ट गाइड
टीईसी ९१००१:२०२२

DRAFT TEST GUIDE
TEC 91001:2022

for

क्वांटम कुंजी वितरण प्रणाली

QUANTUM KEY DISTRIBUTION

(मानको सं.: टीईसी ९१०००:२०२१)
(Standard No.: TEC 91000:2022)

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 : December, 2022

FORWARD

Telecommunication Engineering Centre (TEC) is the technical arm of the 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 Centres (RTECs) have been established, which are located at New Delhi, Bangalore, Mumbai, and Kolkata.

ABSTRACT

This Test Guide provides detailed test schedules and test procedures for evaluating requirements/conformance/functionality/performance of the product against Generic Requirements Standard for the Quantum Key Distribution System (TEC No. 91000:2022).

CONTENTS

A. HISTORY SHEET

Sl. No.	Standard No.	Title	Remarks
1.	TEC No. 91001:2022	Draft Test Guide for Quantum Key Distribution	Release - 1 (Draft) Dec-2022

B. INTRODUCTION

This document describes the testing schedule and procedures for validation of conformance/functionality/requirements/performance of the Quantum Key Distribution (QKD) system against the Generic requirements as per TEC GR No.: 91000:2022.

The manufacturer shall offer his 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.

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.

C. General information for type approval against GR

SN	General Information	Details *(to be filled by testing team)*		
1	Name and Address of the Applicant			
2	Date of Registration of Application			
3	Name and No. of TEC Standard against which the approval sought	TEC standard No: 91000:2022		
4	Topology of QKD System offered for testing	P2P without Relay nodes	P2P with Relay nodes	Multipoint
5	Details of Equipment			
	Type of Equipment	Model No.	Serial No.	
(i)				
(ii)				
(iii)				
(iv)				
(v)				
(vi)				
6	Date of commencement of Tests			
7	Place of Testing			
8	Any other relevant information			
	QKD Protocol(s) supported			

D. Testing team:

TEC Representatives:

S. no.	Name	Designation	Organization	Signature
1.				
2.				
3.				
4.				
5.				
6.				

Manufacturer's Representatives:

S. no.	Name	Designation	Organization	Signature
1.				
2.				
3.				
4.				
5.				

E. List of the Test Instruments:

S.no.	Name of the test instrument	Make /Model	Validity of calibration

F. Equipment Configuration Offered:

(a) <**Equipment/product name**> **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.

(a) <**Other equipment** > **Configuration:**

S.No.	Item	Details	Remarks

G. Equipment/System Manuals:

a) Availability of Installation Manual: **Yes/No**

b) Availability of User Manual: **Yes/No**

c) Availability of Maintenance Manual & Repair Manual etc. **Yes/No**

H. Clause-wise Test Type and Test No.

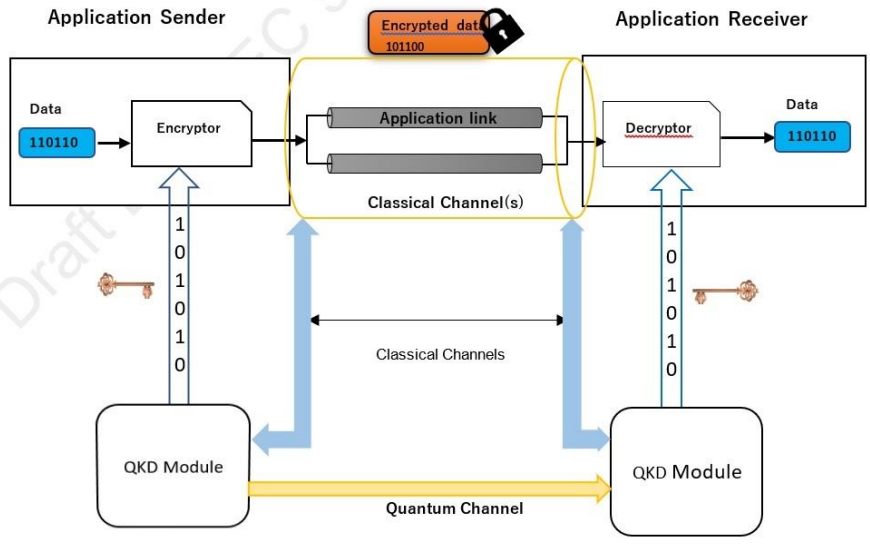
Clause No.	Content of the Clause	Type of Test	Compliance
	CHAPTER 1		
	Technical Requirements		
1.1	**Introduction to QKD Technology:**		
1.1.1	This document describes the generic requirements and specifications for Quantum Key Distribution (QKD) system as per ITU-T Y.3800-3804 Recommendations for use 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.	For information	
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. 	For information	

	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 can happen via existing IP network infrastructure. 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. 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.	For information	
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	For information	

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.

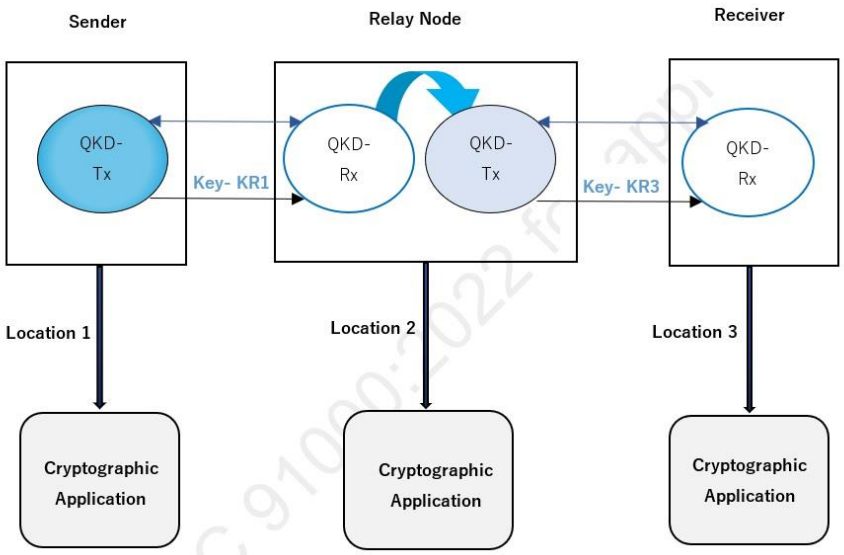
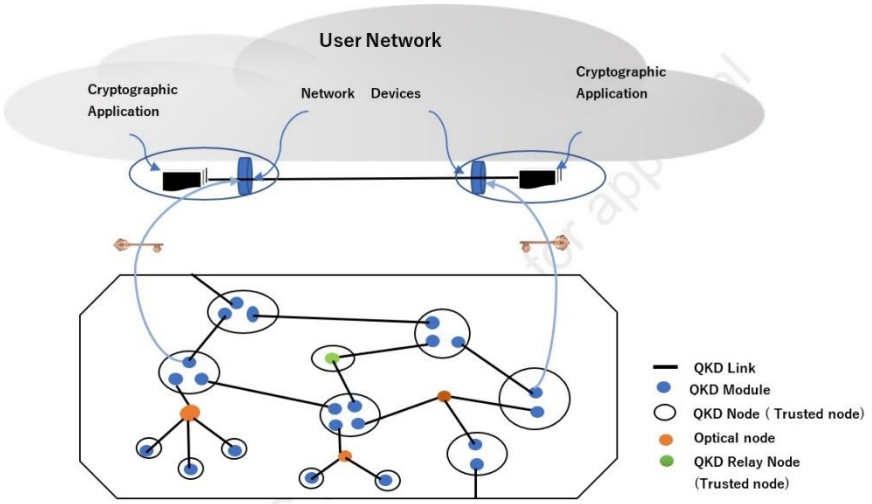


Figure-2 P2P QKD System with Relay Node

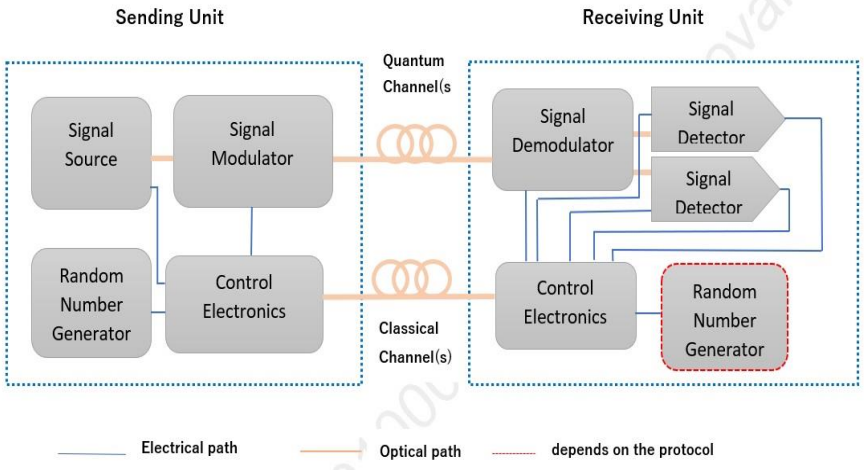
The operating principle of the trusted relay P2P QKD system shown above is explained below.

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 between respectively 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.		
1.1.5	 **Figure-3 Multipoint QKD System** In a multipoint QKD deployment (Figure 3), 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 realizing 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 and Quantum relay nodes are being used for this purpose. Optical switches or splitters can switch or split QKD link traffic between pairs of QKD modules in	For information	

	the multi-point network, to form keys between different users on demand. 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 fiber networks.		
1.1.6	The general characteristics and architecture of offered QKD System shall be compliant to ITU-T Y.3800-3804 series.	Declaration	
1.1.7	The GR outlines the general characteristics of QKD systems including technical requirements for P2P and Multipoint QKD Systems.	For information	
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 and 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.	Declaration	

	 **Figure-4 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 fiber(s)or channel(s). However, there should not be any dependency between the fibers/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.	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 and or single photon source. The Sender unit shall be 19” rack-	Test Case No. 2	

	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, g2(0) must be below <<1.		
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.	Test Case No. 2	
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.	Declaration	
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. 3	
1.5.3	QKD system shall have provision for changing the mean photon number value using an inbuilt Variable Optical Attenuator (VOA).	Test Case No. 4	
1.5.4	QKD systems require multiple single-photon detectors for qubit detection. These detectors should be suitable for use in fiber-optic based QKD systems and shall be able to work either in gated or free running mode. SPD shall be either of the types;	Test Case No. 5	

	(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.	Test Case No. 6	
1.5.6	QKD system shall have provision for changing privacy amplification rate.	Test Case No. 7	
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.	Test Case No. 8	
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.	Declaration	
1.5.9	QKD System shall provide the provision for Discrete Variable (DV) Quantum Key distribution protocol/differentiated phase reference protocols i.e., Coherent One Way (COW), Differential Phase Shift (DPS), etc.	Declaration	
1.5.10	The system shall provide at least one local and remote management interface at each node. The node shall provide a	Test Case No. 9	

	management port for Work Station connectivity with a standard connector.		
1.5.11	The connectors shall be SC/LC/FC/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. 10	
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.	Compliance with an appropriate randomness test report as per the type of source	
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.	Declaration	
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.	Test Case No. 11	
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.	Test Case No. 12	

1.5.16	QKD Modules authentication must be done by a classical channel existing between QKD Modules.	Test Case No. 13	
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.	Test Case No. 14	
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. European Telecommunications Standards Institute (ETSI) defined standards Interface must be used for the transfer of the secret Key.	Test Case No. 15	
1.5.19	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.	Test Case No. 16	
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.	Test Case No. 17	
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.	Test Case No. 18	
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.	Test Case No. 19	
1.5.23	Once Keys are provided by Key Manager to the user network:	Test Case No. 20	

	(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.		
1.6	**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) d. Mean Photon Number e. SPD parameters like dead time, efficiency, etc. f. Quantum channel transmit and receive power g. Real-time monitoring of randomness on-demand h. Key symmetry	Test Case No. 21	
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.	Test Case No. 21	

<table>
<tr><td>1.6.3</td><td>Visibility performance (For COW QKD) over a simulated section shall be tested for 24 hours and visibility performance shall be better than 90%.</td><td>Test Case No. 21</td><td></td></tr>
<tr><td>1.7</td><td>Technical Specifications of QKD System:</td><td></td><td></td></tr>
<tr><td>1.7.1</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>Measure the wavelength of the source using a spectrometer.

Value obtained:</td><td></td></tr>
<tr><td>1.7.2</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</td></tr>
<tr><td colspan="4">>1Kbps for COW protocol</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>Fibre Type</td><td colspan="4">G.652D, G.655, G.657</td></tr>
<tr><td>7.</td><td>Quantum Channel Loss for differential phase reference protocols</td><td>Type of the product</td><td>Short Range</td><td>Long Range</td><td>Extended Range</td></tr>
</table></td><td>Test Case No. 22</td><td></td></tr>
</table>

			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 Requirement 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.					For information	
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.					Test Case No. 23	
1.8.3	The QKD module must provide status information of the QKD module and optionally of the QKD link to the QKDN controller.					Test Case No. 24	
1.8.4	The Key Manager (KM) must 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					Test Case No. 25	

	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.		
1.8.5	The Key Manager must provide fault and performance information of the Key Manager and Key Manager links to the QKDN manager.	Test Case No. 26	
1.8.6	The Key Management unit must include 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.	Test Case No. 27	
1.8.7	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.	Test Case No. 28	
1.8.8	The Key Manager is optionally recommended to support key relays for highly secure encryption like OTP through trusted nodes 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).	Test Case No. 29	
1.8.9	The Key Manager and KM links are Optionally recommended to have capabilities of key synchronization, entity authentication and message authentication to make Key Relaying reliable and secure.	Test Case No. 30	
1.8.10	The Key Managers are optionally recommended to cooperate under the control of the QKDN controller.	Test Case No. 32	
1.8.11	The Key Manager is optionally recommended to present a key supply interface that various cryptographic applications in the	Test Case No. 31	

	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.		
1.8.12	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.	Test Case No. 32	
1.8.13	The QKDN controller must control the status of the key management layer and quantum layer.	Test Case No. 32	
1.8.14	The QKDN controller must control the reconfiguration of the QKD link if failure or eavesdropping occurs.	Test Case No. 32	
1.8.15	The QKDN controller must provide fault, performance, accounting, and configuration information to a QKDN manager.	Test Case No. 32	
1.8.16	The QKDN controller must control KMs and KM links, control of QKD modules and QKD links, authentication and authorization control, etc.	Test Case No. 32	
1.8.17	The QKDN manager must support fault management, accounting management, configuration management, performance management and security management.	Test Case No. 33	
1.8.18	The QKDN manager is required to provision and configures the managed resources in each layer.	Test Case No. 33	
1.8.19	The QKDN manager is optionally recommended to manage the network topology of each layer.	Test Case No. 33	
1.8.20	The QKDN manager is optionally recommended to perform inventory management for all the QKDN resources in each layer.	Test Case No. 33	
1.8.21	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.	Test Case No. 33	

1.8.22	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.	Test Case No. 33	
1.8.23	The QKDN manager is optionally recommended to provide fault detection and root-cause analysis/diagnosis capability for quantum, key management, and QKDN control layers.	Test Case No. 33	
1.8.24	The QKDN manager is optionally recommended to make decisions and generation failure resolving policies and interacts with each layer for correction of faults.	Test Case No. 33	
1.8.25	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.	Test Case No. 33	
1.8.26	The QKDN controller is optionally recommended to provide charging policy control.	Test Case No. 32	
1.8.27	The QKDN controller is optionally recommended to provide session control.	Test Case No. 32	
1.8.28	The QKDN controller is optionally recommended to provide quality of service (QoS) policy control.	Test Case No. 32	
1.8.29	The QKDN controller is optionally recommended to support and ensure access control of functional elements in the quantum layer and the key management layer.	Test Case No. 32	
1.8.30	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. 33	
1.8.31	The QKDN manager must collect the performance data and status of each layer, register them into a performance database and updates them.	Test Case No. 33	
1.8.32	The QKDN manager must analyse the performance of collected data and generates performance reports (Performance Management).	Test Case No. 33	

1.8.33	The QKDN manager must manage the key supply service policies (Performance Management).	Test Case No. 33	
1.8.34	The QKDN manager must collect management information including event logs, audit trails, and so on from each layer for detecting security anomalies.	Test Case No. 33	
1.8.35	The QKDN manager must support key life cycle management by KMs, ensuring traceability of keys by using the log database.	Test Case No. 33	
1.8.36	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.	Test Case No. 33	
1.8.37	The QKDN manager is optionally recommended to manage the key management policies and transmits them to the QKDN controller.	Test Case No. 33	
1.8.38	The QKDN manager is optionally recommended to perform cross-layer management orchestration and also to support management requests from a user network management.	Test Case No. 33	
1.8.39	The QKDN manager must monitor the status of the whole QKDN.	Test Case No. 33	
1.8.40	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.	Test Case No. 33	
1.8.41	The QKDN manager is optionally recommended to provide QoS management and charging management.	Test Case No. 33	
1.8.42	The QKDN manager must detect eavesdropping attempts against a quantum channel.	Test Case No. 33	
1.8.43	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. 33	

1.8.44	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.	Test Case No. 33	
1.8.45	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.	Test Case No. 33	
1.8.46	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.	Test Case No. 34	
1.8.47	The QKDN manager may optionally provide the QKDN resource provisioning requested by the user network manager.	Test Case No. 33	
1.8.48	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. 33	
1.8.49	The QKDN may optionally have the capability to co-operate with the user network either in an integrated or independent management manner.	Check the functionality of the management	
1.8.50	The QKDN must have network control and management capabilities.	Check the network control and management capabilities and the logs generated thereof.	
1.8.51	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.	Verify as per the results of Test Case No. 22	
1.8.52	The QKDN must have the capability to use optical fibre channels or direct free space optical channels for quantum channel networking.	Test Case No. 35	

1.8.53	The QKDN must be capable of automatically authenticating and operating QKD nodes that are rebooted.	Re-boot the system and check whether the authentication of QKD nodes are done.	
1.8.54	The QKDN may have the capability to manage QoS by taking into account the request from the user network.	Test Case No. 36	
1.8.55	The equipment must support Dual stack IP addresses (IPv4 & IPv6) for management and services.	Check the support for IPv4 and IPv6.	
	CHAPTER-2		
	General Requirements		
2.1	**Reference documents**		
2.1.1	Whatever that has not been specifically stated in this document, shall deem to be as per relevant latest ITU-T Recommendations.	For information.	
2.1.2	Relevant ITU-T Recommendations & other specifications are given in the GR.	For information.	
2.1.3	All references to TEC GRs & other Recommendations imply their latest issues.	Declaration	
2.2	**Engineering requirements**		
2.2.1	The manufacturers shall furnish the actual dimensions and weight of the equipment.	Test Case No. 37	
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.	Physical Check	
2.2.3	The system shall work in an environment with 10° C to 25° C temperature and 80% Rh.	Test Case No. 42	
2.2.4	It should be engineered to comply with environmental test requirements as defined in this document.	Test Case No. 42	

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.	Physical check	
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.	Physical check	
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.	Physical check	
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.	Physical check	
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.	Physical check	
2.2.10	Important Do's and Don'ts about the operation of the system shall be indicated.	Physical check	
2.3	**Operational requirements**		
2.3.1	The equipment shall be designed for continuous operation.	Covered in field trial.	
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	
2.3.3	Visual indication to show power ON/OFF status shall be provided.	Physical check	

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.	Test case No. 38	
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.	Report to be submitted.	
2.4.2	The equipment shall be manufactured in accordance with the international quality management system ISO 9001:2015 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.	Declaration/Certificate to be submitted for ISO 9001:2015 compliance. Quality plan describing the quality assurance system may be checked.	
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.	No action required.	
2.5.2	The equipment shall have easy access for servicing and maintenance.	Physical check	
2.5.3	Suitable alarms shall be provided for the identification of faults in the system and faulty units.	Test Case No. 39	
2.5.4	Ratings and types of fuses used are to be indicated by the supplier.	Physical check	

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.	Test Case No. 40	
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. 41	
2.6.3	The equipment shall operate over this range without any degradation in performance.	Test Case No. 41	
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. 41	
2.6.5	The derived DC voltages in the equipment shall have protection against over-voltage, short-circuit and overload.	Test Case No. 41	
2.6.6	The power consumption shall be minimal. The actual power rating/ consumption is to be furnished by the manufacturer of the equipment.	Check the value of power consumption specified by the manufacturer and verify by measuring the power consumption of the system.	
2.7	**Accessories**		
2.7.1	The supplier shall provide a complete set of: a) All the necessary connectors, connecting cables and accessories are required for satisfactory and convenient operation of the equipment. Types of connectors, adapters	Check whether the complete details of the necessary connectors,	

	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.	connecting cables and accessories are required for satisfactory and convenient operation of the equipment are mentioned in the operating manual.	
2.8	**Documentation**		
2.8.1	Technical literature in the English language only shall be accepted.	Check if the document is in English.	
2.8.2	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.	Check whether the Installation, operation and maintenance manual covers the required aspects.	
2.8.3	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.	Check whether the Repair manual 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.	Physical Check	
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.	A test certificate/ test report shall be furnished	
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.	Physical check	
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.	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.	Physical Check	

2.10.5	The equipment shall have a terminal for grounding the rack.	Physical Check	
2.10.6	All switches/controls on the front panel shall have suitable safeguards against accidental operation.	Physical Check	
2.10.7	The equipment shall be adequately covered to safeguard against entry of even dust, insects, etc.	Physical Check	
2.11	**Minimum Equipment offered 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) Multipoint QKD system	Physical Check	
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) 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.	Check on the field along with log report the following system parameters: i. Quantum-Bit Error Rate (QBER) ii. Key Rate	

		iii. Visibility (as applicable to a protocol) iv. Mean Photon Number v. SPAD parameters like dead time, efficiency, etc. vi. Classical channel transmits and receives power vii. Randomness viii. Key Symmetry	
2.13	**Environmental Testing Requirement**		
2.13.1	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**	Test Case No. 42	

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 days: 25 ° C Ambient Temp: 20° C	Rh-95%
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**	Report from TEC accredited test lab to be submitted.	
3.2	**Electromagnetic Interference**	Report from TEC accredited test lab to be submitted.	
3.3	**General Electromagnetic Compatibility (EMC) Requirements**	Report from TEC accredited test lab to be submitted.	

I. Test Setup & Procedures for Testing of Quantum Key Distribution (QKD) System:

(1) Test Case Description for P2P QKD System without Relay Node (Figure 5):

As per figure 5, for communications between Applications connected to QKD Module at Location 1 and QKD Module at Location 2, secure Key K12 is supplied to Cryptographic Applications at location 1 and Location 2. The key should match at both locations. The same needs to be tested both through COW and/or DPS Protocol.

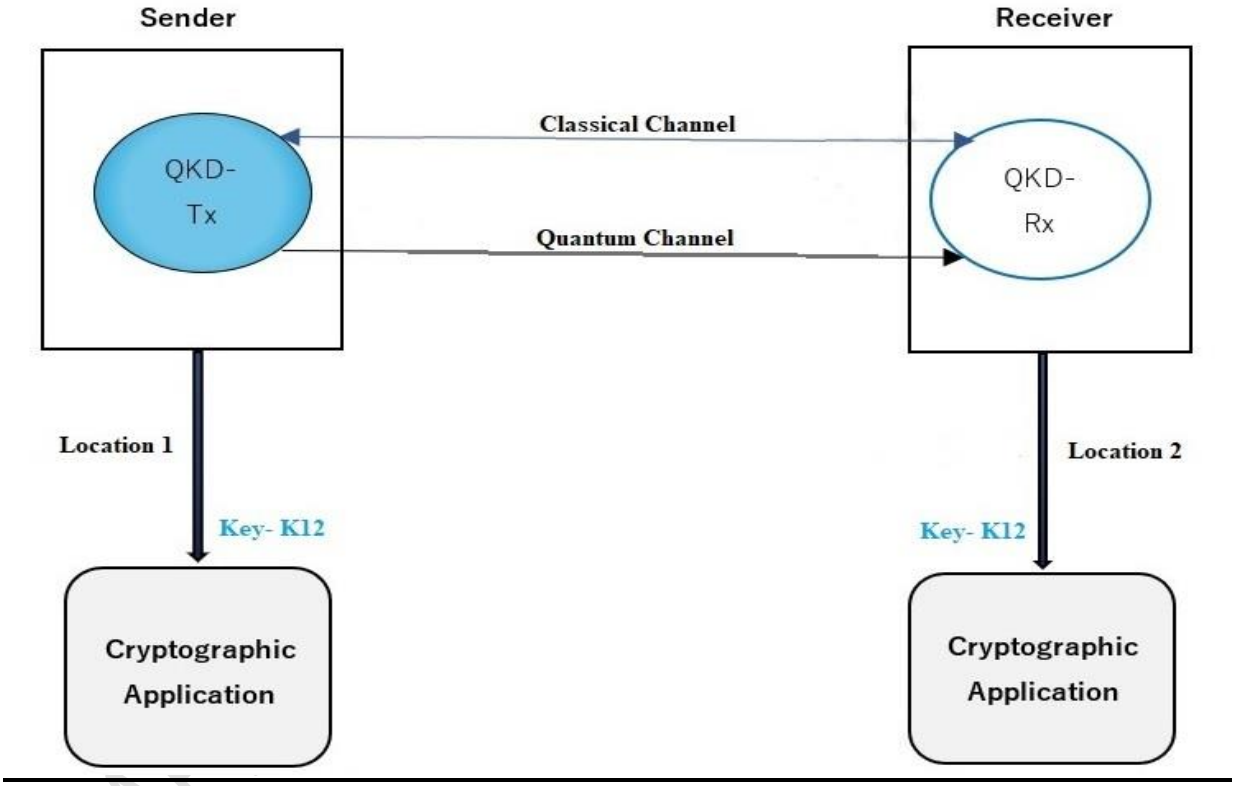


Figure-5: Test setup of P2P QKD System (Without Relay Node)

(2) Test Case Description for P2P QKD System with Relay Node: (Figure 6)

As per figure 6, the QKD relay node (R) is added at an intermediate location for Key Relaying. Secure communication needs to happen between cryptographic applications at Location 1 and Location 2.

QKD Modules at Location '1' and the Intermediate location generate key K1R, QKD Modules at the Intermediate location and Location '2' generates key KR2.

A mathematical function/algorithm shall be used to securely relay the Key at the intermediate office by using both K1R and KR2 so that Location '1' and Location '2' will have the same key (Key K12).

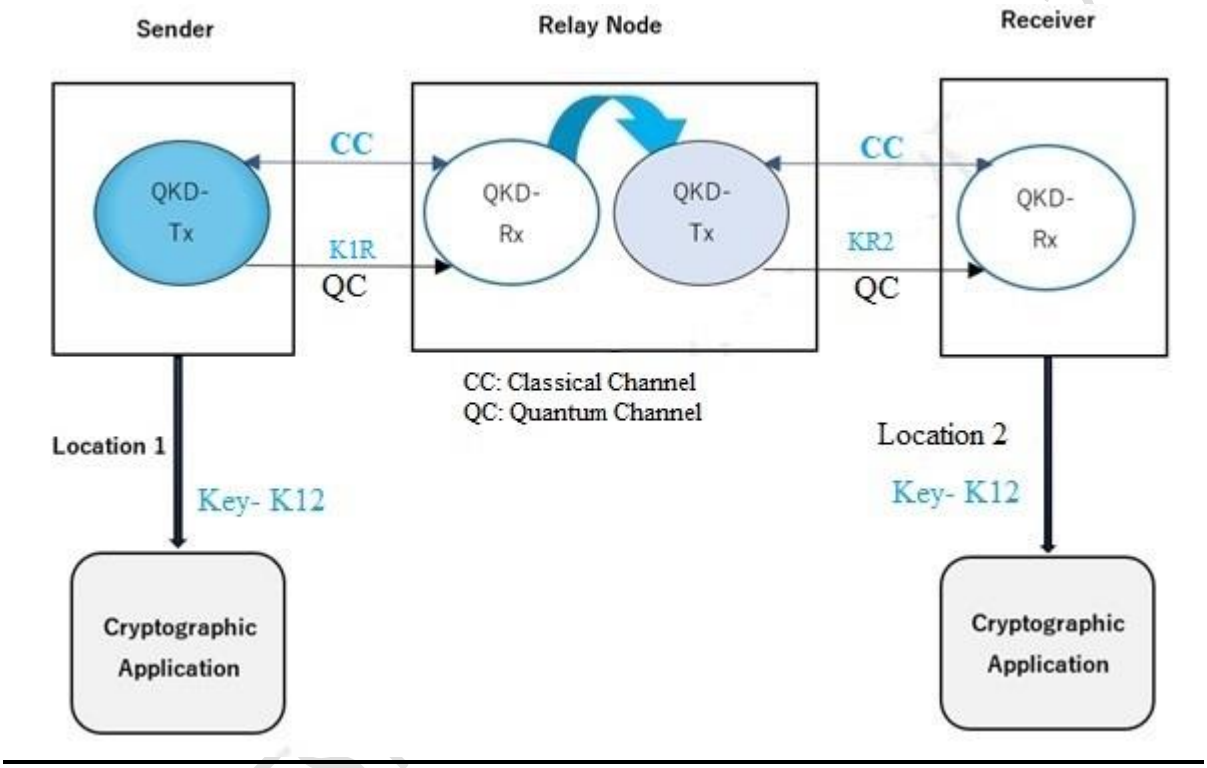


Figure-6: Test setup of P2P QKD System with Relay Node

(3) Test Case Description for Multipoint QKD System: (Figure 7)

As per figure 7, an optical splitter/switch is added for interconnecting one QKD node with more than one QKD node in a time-shared manner for optimally realizing a QKD Network. The optical splitter/switch can switch or split QKD link traffic between pairs of QKD modules in the multi-point network, to form keys between Cryptographic Application-1 at Location 1 and Location 2 and Cryptographic Application-2 at Location 1 and Location 3.

QKD Modules at Location '1' and Location '2' generates key-K12. Similarly, QKD Modules at Location '1' and Location '3' generates key-K13.

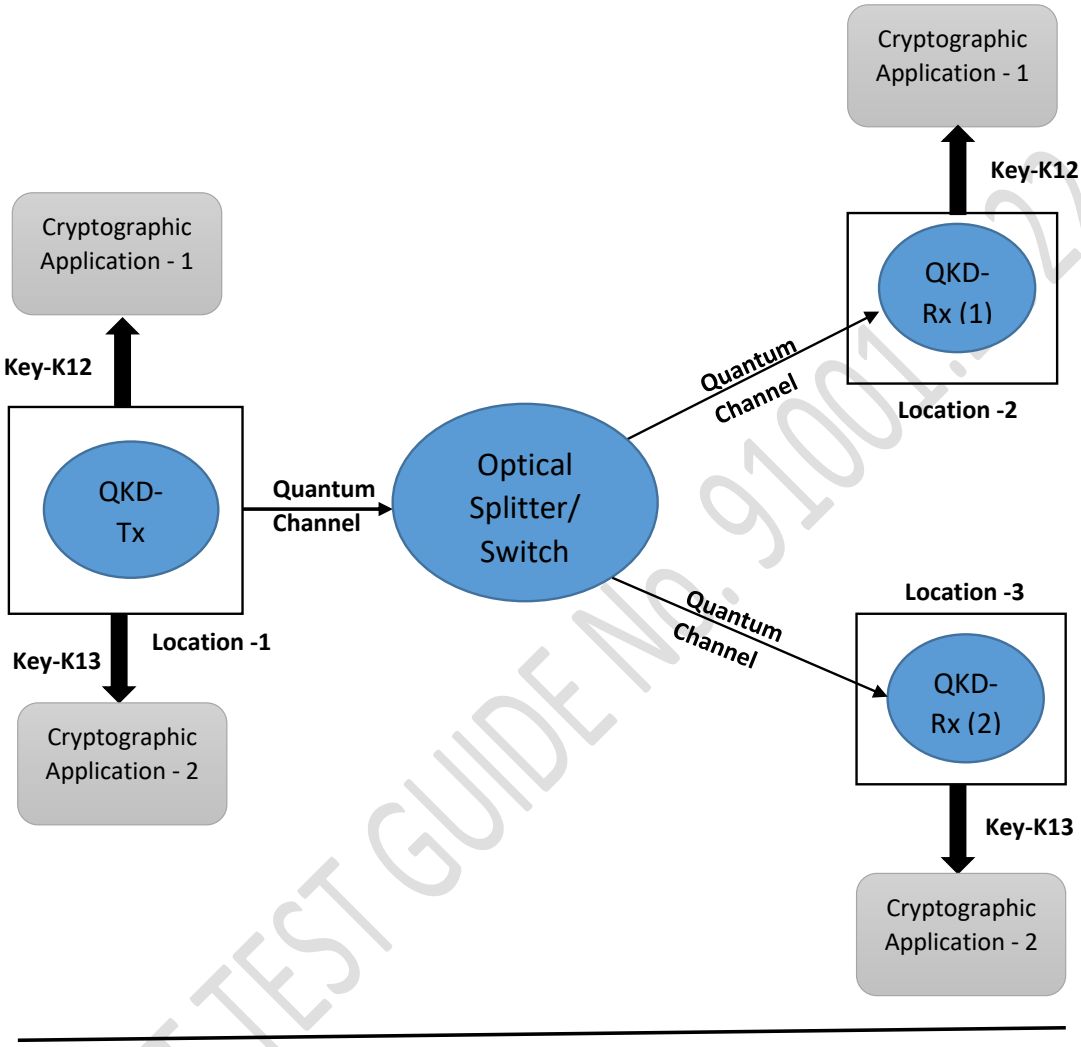


Figure-7: Test setup of Multipoint QKD System

Test Case No. 1

1. Cryptographic Application Interface at QKD-Tx:
2. Cryptographic Application Interface at QKD-Rx:
3. Key sifting: Yes/No
4. Error estimation/correction: (Protocol used)

5. Privacy amplification: (Protocol used and Privacy Amplification Rate)
6. Key management: Yes/No
7. Performance monitoring: Yes/No
8. System configuration and administration: Yes/No
9. Auto-calibration: Yes/No
10. System health parameters: Yes/No

(Note down the parameters being reported for monitoring system health)

Test Case No. 2a

Sender Unit:

1. 19'' Rack Mountable: (Yes/No)
2. Height:
3. Signal Source:
4. Wavelength of Signal Source:
5. Modulation:
6. g2(0) value in case of Single Photon Source:
7. Random Number Generator details:

Test Case No. 2b

Receiver Unit:

1. 19'' Rack Mountable: (Yes/No)
2. Height:

3. Signal detection type:

4. Random Number Generator details:

5. Control Electronics System: Yes/No

Test Case No. 3

Source Intensity of QKD Source:

Photon number probability distribution, p(n) of QKD source:

Test Case No. 4

Mean Photon number value of Source:

Procedure: Change the Mean photon Number value using inbuilt Variable Optical Attenuator (VOA) and verify the Key parameters as below:

S.No.	Parameters	Mean Photo Number [Value 1]	Mean Photo Number [Value 2]	Mean Photo Number [Value 3]
1.	Key Rate			
2.	QBER			
3.	Visibility (as applicable to a protocol)			
4.	SPD parameters like dead time, efficiency, etc.			
5.	Key symmetry			

Test Case No. 5

SPD Type:

Mode of Operation: Gated/ Free Running

Dark count rate:

After Pulse rate:

Jitter:

Dead Time:

Countermeasures against quantum/classical channel attacks:

S.No.	Quantum/classical channel attacks	Countermeasures

Test Case No. 6

Change the Disclose Rate and verify the Key parameters as below:

S.No.	Parameters	Disclose Rate [Value 1]	Disclose Rate [Value 2]	Disclose Rate [Value 3]
1.	Key Rate			
2.	QBER			
3.	Visibility (as applicable to a protocol)			

4.	SPAD parameters like dead time, efficiency, etc.			
5.	Key symmetry			

Test Case No. 7

Change the privacy amplification rate and verify Key parameters as below:

S.No.	Parameters	Privacy Amplification Rate [Value 1]	Privacy Amplification Rate [Value 2]	Privacy Amplification Rate [Value 3]
1.	Key Rate			
2.	QBER			
3.	Visibility (as applicable to a protocol)			
4.	SPAD parameters like dead time, efficiency, etc.			
5.	Key symmetry			

Test Case No. 8

Change the information reconciliation algorithm and the corresponding code rate and verify the Key parameters as below and make sure that the key is tamper-proof.

S.No.	Parameters	Algorithm:		Algorithm:	
		Code Rate [Value 1]	Code Rate [Value 2]	Code Rate [Value 1]	Code Rate [Value 2]

1.	Key Rate				
2.	QBER				
3.	Visibility (as applicable to a protocol)				
4.	SPAD parameters like dead time, efficiency, etc.				
5.	Key symmetry				

Test Case No. 9

Type of Local / Remote management Interface at Sender Unit:

Type of Local / Remote management Interface at Receiver Unit:

Conduct and verify a few tests to check the functioning of Local and Remote Management Interface.

Observations:

Test Case No. 10

Sender Unit:

Sl .No.	Optical Connector Interface at Sender Unit	Interface Type (SC/LC/FC/ST)	Return Loss

Receiver Unit:

Sl .No.	Optical Connector Interface at Receiver Unit	Interface Type (SC/LC/FC/ST)	Return Loss

Physically check the requirements of the connector as given below:

a) provision of automatic shutters having spring action or provision of closing them manually. [Yes/No]
b) When out-of-use, they shall remain closed. [Yes/No]
c) the optical connectors shall be so positioned as be leaning towards the ground to avoid direct laser beam incidence on the user. [Yes/No]

Test Case No. 11

Sl. No.	Description	QKD Parameters	Key delivery (Yes/No)
1	Current QKD System Date and Time:	QBER : Key Rate:	
2	Change QKD system time as Leap Year:	QBER : Key Rate:	
3	Change QKD system time as Millenium / Century (1900 / 2300 /5000):	QBER: Key Rate:	

Test Case No. 12

	Measured Power through wide-band Optical Power Meter for Classical Channel	**Optical Power as per QKDN Manager for Classical Channel**	**Measurement Accuracy**	**Measurement Accuracy as prescribed by NIST**
Input Power				
Output Power				

Test Case No. 13

1. Verify the Authentication status of QKD Modules for COW Protocol

Observations:

2. Verify the Authentication status of QKD Modules for DPS Protocol

Observations:

Test Case No. 14

Sl. No.	Functions of QKD Protocols	Status of Implementation		Remarks
		Sender Unit	Receiver Unit	

1	Random number generation			
2	Quantum Key Transfer			
3	Distillation for key generation			
4	Quantum channel synchronization			

Test Case No. 15

P2P QKD System without Relay Node:

Type of Interface for Key Transfer:

	Key Generated (Yes/No)	**Key delivered to the Key Manager (Yes/No)**	**Remarks**
QKD module at the sender node			
QKD module at the receiver node			

P2P QKD System with Relay Node:

Type of Interface for Key Transfer:

	Key Generated (Yes/No)	**Key delivered to the Key Manager (Yes/No)**	**Remarks**
QKD module at the sender node			

QKD-Rx module at the relay node 1			
QKD-Tx module at the relay node 1			
QKD module at the receiver node			

Test Case No. 16

Procedure: Check the status request message sent by the Key Manager to the QKD module and the status information response received from the QKD module.

Command message for Status Information Supply:

Item	Description	Remarks
Message ID	A message identifier generated by a KM for the command message for status information supply	
Command Code	A code that indicates the command message is used for status information supply.	
Sender ID	Unique ID of the KM sending the command message for status information supply.	
Period	A time interval of status information supply requested by the KM.	
Status Table	A table of parameters requested by the KM.	

Response message for Status Information Supply:

Item	Description	Remarks
Message ID	A message identifier generated by QKD module for the response message for status information supply.	
OrigMessage ID	A message identifier received from a command message for status information supply. (Not applicable for a proactive status information supply)	
Command code	A code that indicates the response message is used for status information supply.	
Sender ID	Unique ID of the QKD module sending the response message for status information supply.	
Status Table	A table of status information of parameters supplied by the QKD module sending the response message for status information supply. The parameters may be the corresponding ones requested by the QKDN controller.	
Response code	A code that indicates a result of status information supply. (Success/Failure)	

Observations:

	Status Information obtained from the above procedure	**Status as shown at QKD System**

QKD module status		
QKD-KM link status		

Test Case No. 17

Sl. No.	QBER Threshold Value	Actual value of QBER	QBER value exceeded Threshold (Yes/No)	Alarm reported to user (Yes/No)	Remarks

Test Case No. 18

Note down the following information from the generated key file.

Sl. No.	Elements of Key life cycle management	Value 1	Value 2	Value 3	Remarks
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				

Test Case No. 19

1. Verify the key file format stored in the QKD system as per the details below:

Key File Format:

Item	Description	Remarks
(1) QKD - key		
QKD-key ID	ID of the QKD-key	**M**
Key length	Key length of the QKD-key	
QKD module ID	ID of the QKD module (Alice or Bob) that generates the QKD-key	
Matching QKD module ID	ID to identify the matching QKD module which constitutes the pair of Alice and Bob	
Generation time stamp	Time stamp of QKD-key generation at the pair of QKD modules.	
Hash value	Hash value of the QKD-key data.	
(2) Key Management Agent (KMA) – Key (if applicable)		
KMA-key ID	ID of the KMA-key, which is the same for the pair of keys for Alice and Bob, and unique in a QKD network. A part of the bits of the hash value generated from the names of the pair	**M**

	of QKD modules is often used for this ID.	
Key length	Key length of the KMA-key	
Key type	Index to specify either encrypting key or decrypting key	
KMA ID	ID of the KMA that stores the KMA-key	
Matching KMA ID	ID of the matching KMA	**M**
Generation time stamp	Time stamp of the KMA-key generation at the KMA	
QKD module ID	ID to identify the QKD module which generates the QKD-key corresponding to the KMA-key data	
Matching QKD module ID	ID to identify the matching QKD module which constitutes the pair of Alice and Bob	
Hash value	Hash value of the KMA-key data.	
(3) Relayed KMA-key (for P2MP systems)		
Source KMA ID	ID of source KMA of the key relay	
Destination KMA ID	ID of destination KMA of the key relay	
Key relay time stamp	Time stamp of the key relay	
Key relay encryption method	Encryption method used for the key relay	
KMA-key metadata	Metadata of KMA-key of the source KMA	**M**
(4) KSA - key		
KSA-key ID	ID of the KSA-key	**M**
Key length	Key length of the KSA-key	

Supply time stamp	Time stamp of the KSA-key supply from the KSA to a cryptographic application	
Application name	Name of cryptographic application	
Application source ID	Source ID of cryptographic application	
Application destination ID	Destination ID of cryptographic application	

2. Verify the key deletion functionality as per the details below:

Command message for key deletion:

Item	Description	Remarks
Message ID	A message identifier generated by a cryptographic application for the command message for key deletion.	
Command Code	A code that indicates the command message is used for key deletion.	
Sender ID	Unique ID of the cryptographic application sending the command message for key deletion.	
Source ID	An identifier of a KM to receive the command message for key deletion. ID of the cryptographic application sending the command message for key deletion can be used as Source ID.	

Response code	A code that indicates an authentication result.	
Target ID	An identifier of a KM corresponding to a matching cryptographic application of the cryptographic application sending the command message for key deletion. (ID of the matching cryptographic application can be used as Target ID.)	
Session ID	Unique ID of a key supply session.	
Application code	A code that indicates how keys are consumed. (Encryption/ Deletion)	

Response message for key deletion:

Item	Description	Remarks
Message ID	A message identifier generated by a KM for the response message for key deletion.	
OrigMessage ID	A message identifier received from a command message for key deletion.	
Command Code	A code that indicates the response message is used for key deletion.	
Sender ID	Unique ID of the KM sending the response message for key deletion.	
Source ID	Same as that of the received command message for key deletion.	
Target ID	Same as that of the received command message for key deletion.	

Session ID	Same as that of the received command message for key deletion.	
Application code	Same as that of the received command message for key deletion.	
Response code	A code that indicates a key deletion result. (success/failure)	

Observations:

Sl. No.	Functions of key management policy	Status	Remarks
1	Deletion of Key		
2	Preservation of Key		

Test Case No. 20

Command message for key supply:

Item	Description	Remarks
Message ID	A message identifier generated by a cryptographic application for the command message for key supply.	
Command Code	A code that indicates the command message is used for key supply.	
Sender ID	Unique ID of the cryptographic application	

	sending the command message for key supply.	
Source ID	An identifier of a KM to receive the command message for key supply. (ID of the cryptographic application sending the command message for key supply can be used as Source ID.)	
Target ID	An identifier of a KM to supply keys for a matching cryptographic application of the cryptographic application sending the command message for key supply. (ID of the matching cryptographic application can be used as Target ID.)	
Session ID	Unique ID of a key supply session.	
Application code	A code that indicates how keys are to be consumed. (Encryption/Decryption)	
Key amount	An amount of keys requested by the cryptographic application sending the command message for key supply.	
Key ID	An identifier of a key requested by the cryptographic application sending the command message for key supply	

Response message for key supply:

Item	**Description**	**Remarks**
Message ID	A message identifier generated by a KM for the response message for key supply.	
OrigMessage ID	A message identifier received from a command message for key supply.	

Command Code	A code that indicates the response message is used for key supply.	
Sender ID	Unique ID of the KM sending the response message for key supply.	
Source ID	Same as that of the received command message for key supply.	
Target ID	Same as that of the received command message for key supply.	
Session ID	Same as that of the received command message for key supply.	
Application code	Same as that of the received command message for key supply.	
Key amount	Same as that of the received command message for key supply.	
Key size	Same as that of the received command message for key supply.	
Key ID	Same as that of the received command message for key supply.	
Count ID	An identifier that indicates the number of a serial of sub-sessions of a key supply session. (The requested amount of keys can be supplied through multiple subsessions within one key supply session)	
Key data	Keys supplied by the KM sending the response message for key supply.	
Response code	A code that indicates the status of key supply. (0x01: success, 0x02: sufficient, 0x03: insufficient 0x04: status table)	

Observations:

Sl. No.	Activity performed on Key	Status	Remarks
1	Key request received by Key manager		
2	Key supply by Key manager		

Security Capabilities at the Key-Supply Interface:

S.No	Security Capabilities	Observations

Test Case No. 21

Performance Monitoring:

Sl. No.	Performance Parameters	Threshold value (if applicable, as per GR)	Value of Parameters (Local Monitoring)	Value of Parameters (Remote Monitoring)	Remarks

1	Quantum Bit Error Rate (QBER)				
2	Key Rate				
3	Visibility (as applicable to a protocol)				
4	Mean Photon Number				
5	SPD parameters like dead time, efficiency, etc.				
6	Quantum channel transmit and receive power				
7	Randomness				
8	Key Symmetry				

Test Case No. 22

Verify the Communication protocol and data format for a quantum key distribution (QKD) network to supply cryptographic keys to an application entity (router/switch, etc.) as per ETSI GS QKD 014 V1.1.1 (2019-02). **(Refer Annexure-A)**

Sl. No.	**Specification Description**	**Specified Value**	**Measured value**
1	Secure Key Rate	>2Kbps for DPS protocol	
		>1Kbps for COW protocol	

2	QBER Value along with distance mentioned		<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 phase differential reference protocols	Type of the product	Short Range	Long Range	Extended Range	
		Application	<50 km	50-80 km	>80 km	
		Channel Loss	12dB	18dB	23dB	
	Measured Value at maximum Channel loss	QBER				
		Key Rate				
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			

Test Case No. 23

QKD Link Identifier	Sending Node	Receiving Node	Protocol used

Test Case No. 24

Procedure: Check the status request message sent by the QKDN Controller to the QKD module and the status information response received from the QKD module.

Command message for Status Information Supply:

Item	Description	Remarks
Message ID	A message identifier generated by a QKDN controller for the command message for status information supply	
Command Code	A code that indicates the command message is used for status information supply.	
Sender ID	Unique ID of the QKDN controller sending the command message for status information supply.	
Period	A time interval of status information supply requested by the QKDN controller.	
Status Table	A table of parameters requested by the QKDN controller.	

Response message for Status Information Supply:

Item	Description	Remarks
Message ID	A message identifier generated by a QKD module for the response message for status information supply.	
OrigMessage ID	A message identifier received from a command message for status information supply. (Not applicable for a proactive status information supply)	
Command code	A code that indicates the response message is used for status information supply.	
Sender ID	Unique ID of the QKD module sending the response message for status information supply.	
Status Table	A table of status information of parameters supplied by the QKD module sending the response message for status information supply. The parameters may be the corresponding ones requested by the QKDN controller.	
Response code	A code that indicates a result of status information supply. (Success/Failure)	

Status Information obtained from the above procedure:

Test Case No. 25

Procedure: Check the status request message sent by the QKDN Controller to the Key Manager and the status information response received from the Key Manager.

Command message for Status Information Supply:

Item	Description	Remarks
Message ID	A message identifier generated by a QKDN controller for the command message for status information supply	
Command Code	A code that indicates the command message is used for status information supply.	
Sender ID	Unique ID of the QKDN controller sending the command message for status information supply.	
Period	A time interval of status information supply requested by the QKDN controller.	

Status Table	A table of parameters requested by the QKDN controller. The parameters 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.	

Response message for Status Information Supply:

Item	Description	Remarks
Message ID	A message identifier generated by a KM for the response message for status information supply.	
OrigMessage ID	A message identifier received from a command message for status information supply. (Not applicable for a proactive status information supply)	
Command code	A code that indicates the response message is used for status information supply.	
Sender ID	Unique ID of the KM sending the response message for status information supply.	
Status Table	A table of status information of parameters supplied by the KM sending the response message for status information supply. The parameters may be the corresponding ones requested by the QKDN controller.	

Response code	A code that indicates a result of status information supply. (Success/Failure)	

Status Information obtained from the above procedure:

Test Case No. 26

Check the status request message sent by the QKDN Manager to the Key Manager (if status information is not automatically sent by Key Manager) and the status information response received from the Key Manager.

Status Information available at the QKDN Manager:

Test Case No. 27

Check the hardware module where the generated keys are stored and verify the following:

Maximum Key size that can be stored: _____

Maximum Length of the key supplied by Key Manager:_____

Verify the QKD system for variable key lengths output i.e. 32/64/128/256/512 bits.

S.No.	Name of the Cryptographic Application	Key-size	Key Delivered (Y/N)	Remarks
1.		32		
2.		64		
3.		128		
4.		256		
5.		512		

Test Case No. 28

Sl. No.	Activity performed by Key Manager	Status	Remarks
1.	Key re-size		
2.	Key re-format (necessary headers and footers such as key ID, generation date, key length, etc., for key management)		
3.	Key Storage		

4.	QKD Link Parameters: a) QBER b) Key Rate c) Link Status		
5.	Formatting of Keys where lengths for key supply are not appropriate.		

Test Case No. 29

Sl. No.	Source KM	Destination KM	Key Relay Time Stamp	Key Relay Encryption Method
1.				
2.				
3.				
4.				
5.				

Test Case No. 30

Sl. No.	Capabilities to be supported by Key Manager	Observations
1.	Key Synchronization	
2.	Entity Authentication	
3.	Message Authentication	

Test Case No. 31

Key Supply Interface: _____

Verify the authentication/access control between the Key Manager and the Cryptographic application as per the details below:

Command message for Authentication:

Item	Description	Remarks
Message ID	A message identifier generated by a sender of the command message for authentication.	
Command Code	A code that indicates the command message is used for authentication.	
Sender ID	Unique ID of the sender of the command message for authentication.	
Authentication info	Information used for authentication. The authentication information is configurable and may be generated by algorithms.	

Response message for Authentication:

Item	Description	Remarks
Message ID	A message identifier generated by a sender of the response message for authentication.	
OrigMessage ID	A message identifier received from a command message for authentication.	
Command code	A code that indicates the response message is used for authentication	

Sender ID	Unique ID of the sender of the response message for authentication (Success/ Failure)	
Response code	A code that indicates an authentication result.	

Test Case No. 32

Sl. No.	Functions of QKD Controller	Observations
1.	Key relay Route control (including rerouting) bases on request from service layer	
2.	Controlling the status of Key management layer and Quantum layer	
3.	Reconfiguration of the QKD link in case of failure or eavesdropping	
4.	Providing fault, performance, accounting, and configuration information to a QKDN manager	
5.	KMs and KM links control	
6.	QKD Module Control	
7.	OKD Link Control	
8.	Authentication and Authorization Control of the functional elements in the Quantum layer and Key Management Layer	

9.	Charging policy control	
10.	Session control	
11.	Quality of Service (QoS) policy control	

Test Case No. 33

Sl. No.	Functions/Capability of QKD Manager	Observations
1.	Fault management	
2.	Accounting management	
3.	Configuration management	
4.	Performance management	
5.	Security Management	
6.	Inventory management for the QKDN resources in each layer	
7.	Life cycle management of the resource repositories	
8.	Provisioning and configuration of managed resources in each layer (e.g., create, store, retrieve, modify, remove, etc.) in each layer.	

9.	Monitoring of resource data usage of each layer	
10.	Generation of account policies for charging	
11.	Management of Network Topology	
12.	Monitoring of QKD Link failure	
13.	Reconfiguration of QKD links	
14.	Rerouting of key relay routes	
15.	Fault detection and root-cause analysis/diagnosis capability for quantum key management, and QKDN control layers.	
16.	Decision and generation of failure resolving policies and interaction with each layer for correction of faults.	
17.	Bootstrapping policies to make the resources ready for the operation	
18.	Collection of performance data and status of each layer and registering into a performance database and updating it.	
19.	Analysis of performance database and generation of Performance Report	

20.	Management of Key supply service policies	
21.	Collection of management information including event logs, audit trails, and so on from each layer for detecting security anomalies.	
22.	Traceability of keys by using the log database	
23.	Provision of Root certification authority for issuing root certificates to the QKDN controller	
24.	Access control of QKDN Controller	
25.	Management of key management policies and transmitting them to the QKDN controller	
26.	Perform cross-layer management orchestration	
27.	Support management requests from a user network management.	
28.	Monitoring the status of whole QKDN	
29.	Management of the identification and registration of modules in a QKDN, and their access rights	
30.	QoS management and charging management.	
31.	Detection of eavesdropping attempts against a quantum channel.	

32.	Provide availability and reliability of quantum key distribution based on the redundancy of QKD links provided by the quantum layer.	
33.	Managing the routing and rerouting of key relays by the QKDN controller in the event of faults or performance degradation	
34.	QKDN resource provisioning requested by the user network manager.	
35.	Provision of 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. 34

Sl. No.	**Module Channel**		**Unique Identifier**
1.	Classical Channel		
2.	Quantum Channel		
3.	**Node Details:**	**Details of Module in the Node:**	

	Node Details:	**Details of Module in the Node:**	
	--		

Verify that the unique identifier is used in key routing and key relays.

Observations:

Test Case No. 35

Sl. No.	Performance parameters	Optical Fiber Channel	Free Space Optical Channel	Remarks
1.	Key Rate			
2.	QBER			
3.	<Any other parameter>			

Test Case No. 36

Deteriorate the normal operating conditions (insert loss in the channel, etc.) and check the response of the system.

Sl. No.	Operating Conditions	Response of the system for managing QoS	System parameters (Key Rate, QBER, etc.)	Remarks

Test Case No. 37

Sl. No.	QKD Module	Length (In mm)	Width (In mm)	Depth (In mm)	Weight (In Kg)
1.	QKD Sender Unit				
2.	QKD receiver Unit				
3.	QKD-Rx Unit (Relay Node)				
4.	QKD-Tx Unit (Relay Node)				

Test Case No. 38

Visual Indicators on Sender Module:

Sl. No.	Visual Indicator Details	Colour Coding used	Observations

Visual Indicators on Receiver Module:

Sl. No.	Visual Indicator Details	Colour Coding used	Observations

Test Case No. 39

Note down the defined alarms in the system. Further, create alarms and clear them.

Sl. No.	Alarm Name	Interface	Descriptions	Alarm Reporting Status on QKD System GUI	Alarm clear Status

Test Case No. 40

Power supply Details for QKD System

Test Case No. 41

Sl. No.	Variation in the Power Supply	QKD System Performance Parameters (Key Rate, QBER, Key Symmetry, etc.)	Remarks
1.	Increase the AC mains supply of 230V by +10%		
2.	Decrease the AC mains supply of 230V by -15%		
3.	Increase the frequency of AC supply by 2 Hz to 52 Hz		

4.	Decrease the frequency of AC supply by 2 Hz to 48 Hz		
5.	Vary the DC supply of -48V in the range from -40V to -60V		

Verify whether the instrument is adequately protected by varying the voltage variation beyond the range mentioned above and by also reversing the input polarity in case of DC feed and in the event of over-voltage, short-circuit and overload.

Observations:

Test Case No. 42

Carry out environment tests according to the cycle mentioned in TEC SD: QM-333 and measure the key-rate and QBER during the functional check.

S. N.	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 days: 25 ° C Ambient Temp: 20° C	Rh-95%
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%

Additional tests

S.No	Procedure	Expected Result	Actual Result	Remarks
1	Check the working QKD protocol on web GUI.	Web GUI should display the used protocol of QKD module.		
2	Download/Activate the new system software through GUI	Download / Activate software should be successful.		
3	View the software version through the GUI	Information regarding all the versions of software present to be shown at GUI In case multiple versions, one is active and the other version is in idle (passive) mode.		
4	Check the optical parameters for QKD modules.	Web GUI should display the Optical parameters.		
5	Check the optical parameters of the Classical Channel.	Web GUI should display the optical parameters of the Classical Channel.		
6	Verify system reboot feature through GUI	QKD System shall be rebooted		

Annexure-A: Protocol and data format of REST-based key delivery API as per ETSI GS QKD 014 V1.1.1 (2019-02)

1. Protocol Specifications:

1.1. Common Specification:

The common specification is as follows.

Name	Description
Communication Protocol	HTTPS
Character code	UTF-8
HTTP Content-type	application/json

The list of API methods shall be as follows.

No.	Method name	URL	Access Method
1	Get status	https://{KME_hostname}/api/v1/keys/{slave_SAE_ID}/status	GET
2	Get key	https://{KME_hostname}/api/v1/keys/{slave_SAE_ID}/enc_keys	POST (or GET)
3	Get key withkey IDs	https://{KME_hostname}/api/v1/keys/{master_SAE_ID}/dec_keys	POST (or GET)

1.2. Get status

The specification of the "Get status" method shall be as follows.

Name	Description		
Overview	Returns **Status** from a KME to the calling SAE. **Status** contains information on keys available tobe requested by a master SAE for a specified slave SAE.		
Access method	GET		
Access URL	https://{KME_hostname}/api/v1/keys/{slave_SAE_ID}/status		
Parameters	Name	Data type	Description
	{KME_hostname}	String (in URL)	Hostname or IP address of the KME. A port number may be specified separated from the hostname or IP address by a colon
	{slave_SAE_ID}	String (in URL)	URL-encoded SAE ID of slave SAE
Request data model (from SAE toKME)	None.		
Response data model (from KMEto SAE)	**Status** (see clause 6)		
Pre-condition	None.		
Post-condition	None.		

Get status may return error responses as follows.

HTTP status code	Response data model	Description
400	**Error**	Bad request format.
401	-	Unauthorized.
503	**Error**	Error on server side.

1.3. Get key

The specification of the "Get key" method shall be as follows.

Name	Description		
Overview	Returns **Key container** data from the KME to the calling master SAE. **Key container** data contains one or more keys. The calling master SAE may supply **Key request** data to specifythe requirement on **Key container** data. The slave SAE specified by the slave_SAE_ID parameter may subsequently request matching keys from a remote KME using key_ID identifiers from the returned **Key container**.		
Access method	POST (or GET for specified simple requests only (see clause 6))		
Access URL	https://{KME_hostname}/api/v1/keys/{slave_SAE_ID}/enc_keys		
Parameters	Name	Data type	Description
	{KME_hostname}	String (in URL)	Hostname or IP address of the KME. A port number may be specified separated from the hostname or IP address by a colon
	{slave_SAE_ID}	String (in URL)	URL-encoded SAE ID of slave SAE
Request data model(from SAE to KME)	**Key request** (POST only; see clause 6)		
Response data model(from KME to SAE)	**Key container** (see clause 6)		
Pre-condition	None.		
Post-condition	Requested number of keys provided to SAE are removed from key pool stored in KME.		

The "Get key" method may return error responses as follows.

HTTP status code	Response data model	Description
400	**Error**	Bad request format.
401	-	Unauthorized.
503	**Error**	Error on server side.

1.4. Get key with key IDs

The specification of the "Get key with key IDs" method shall be as follows.

Name	Description

Overview	Returns **Key container** from the KME to the calling slave SAE. **Key container** contains keysmatching those previously delivered to a remote master SAE based on the **Key IDs** suppliedfrom the remote master SAE in response to its call to Get key. The KME shall reject the request with a 401 HTTP status code if the SAE ID of the requestorwas not an SAE ID supplied to the "Get key" method each time it was called resulting in the return of any of the **Key IDs** being requested.		
Access method	POST (or GET for specified simple requests only (see clause 6))		
Access URL	https://{KME_hostname}/api/v1/keys/{master_SAE_ID}/dec_keys		
Parameters	Name	Data type	Description
	{KME_hostname}	String (in URL)	Hostname or IP address of the KME. A port number may be specified separated from the hostname or IP address by a colon
	{master_SAE_ID}	String (in URL)	URL-encoded SAE ID of master SAE
Request data model(from SAE to KME)	**Key IDs** (POST only; see clause 6)		
Response data model (from KME toSAE)	**Key container** (see clause 6)		
Pre-condition	None.		
Post-condition	Specified keys by Key IDs provided to SAE are removed from key pool stored in KME.		

The "Get key with key IDs" method may return error responses as follows.

HTTP status code	Response data model	Description
400	**Error**	Bad request format.
401	-	Unauthorized.
503	**Error**	Error on server side.

2. Data Format Specifications:

2.1. Status data format

Status data format is used for a response data model of API "Get status" method.

JSON data format of Status shall be as follows.

Items	Data type	Description
source_KME_ID	string	KME ID of the KME
target_KME_ID	string	KME ID of the target KME
master_SAE_ID	string	SAE ID of the calling master SAE
slave_SAE_ID	string	SAE ID of the specified slave SAE
key_size	integer	Default size of key the KME can deliver to the SAE (in bit)
stored_key_count	integer	Number of stored keys KME can deliver to the SAE
max_key_count	integer	Maximum number of stored_key_count
max_key_per_request	integer	Maximum number of keys per request
max_key_size	integer	Maximum size of key the KME can deliver to the SAE (in bit)

min_key_size	integer	Minimum size of key the KME can deliver to the SAE (in bit)
max_SAE_ID_count	integer	Maximum number of additional_slave_SAE_IDs the KME allows. "0" when theKME does not support key multicast
status_extension	object	(Option) for future use

An example of Status data format is as follows.

```
{
    "source_KME_ID":          "AAAABBBBCCCCDDDD",
    "target_KME_ID":          "EEEEFFFFGGGGHHHH",
    "master_SAE_ID":          "IIIIJJJJKKKKLLLL",
    "slave_SAE_ID":           "MMMMNNNNOOOOPPPP",

    "key_size": 352,

    "stored_key_count": 25000,

    "max_key_count": 100000,
}
```

3. Key request data format

Key request data format is used for a request data model of API "Get key" method. JSON data format of Key request shall be as follows.

Items	Data type	Description
number	integer	(Option) Number of keys requested, default value is 1.
size	integer	(Option) Size of each key in bits, default value is defined as key_size inStatus data format.
additional_slave_SAE_IDs	array of strings	(Option) Array of IDs of slave SAEs. It is used for specifying two or more slave SAEs to share identical keys. The maximum number of IDsis defined as max_SAE_ID_count in Status data format.
extension_mandatory	array of objects	(Option) Array of extension parameters specified as name/value pairsthat KME shall handle or return an error. Parameter values may be ofany type, including objects.
extension_optional	array of objects	(Option) Array of extension parameters specified as name/value pairsthat KME may ignore. Parameter values may be of any type, includingobjects.

Examples of Key request data format is as follows:

```
{
    "number":
    3,
}



    "number": 1,

    "size": 4096,
    "additional_slave_SAE_IDs":
    [
}



    "number": 20,

    "size": 512,
    "extension_mandatory"
    : [

        {

            "abc_route_type":
            "direct"

        },

        {
}
```

3.1. Key container data format

Key container data format is used for a response data model of API "Get key" method and "Get key with key IDs" method. JSON data format of Key container shall be as follows.

Items		Data type	Description
Keys		array of objects	Array of keys. The number of keys is specified by the "number" parameter in "Get key". If not specified, the defaultnumber of keys is 1.
	key_ID	string	ID of the key: UUID format (example: "550e8400-e29b-41d4-a716-446655440000").
	key_ID_extension	object	(Option) for future use
	key	string	Key data encoded by base64 [7]. The key size is specified bythe "size" parameter in "Get key". If not specified, the "key_size" value in Status data model is used as the defaultsize.
	key_extension	object	(Option) for future use.
key_container_extension		object	(Option) for future use.

An example of Key container data format is as follows.

```
{
     "keys": [

          {

             "key_ID": "bc490419-7d60-487f-adc1-4ddcc177c139",
             "key": "wHHVxRwDJs3/bXd38GHP3oe4svTuRpZS0yCC7x4Ly+s="

         },

         {

             "key_ID": "0a782fb5-3434-48fe-aa4d-14f41d46cf92",
             "key": "OeGMPxh1+2RpJpNCYixWHFLYRubpOKCw94FcCI7VdJA="

         },

         {
}
```

3.2. Key IDs data format

Key IDs data format is used for a request data model of API "Get key with key IDs" method. JSON data format of Key IDs shall be as follows.

Items		Data type	Description
key_IDs		array of objects	Array of key IDs
	key_ID	string	ID of the key: UUID format (example: "550e8400-e29b-41d4-a716-446655440000")
	key_ID_extension	object	(Option) for future use
key_IDs_extension		object	(Option) for future use

An example of Key IDs data format is as follows.

```
{
    "key_IDs": [

         {

             "key_ID": "bc490419-7d60-487f-adc1-4ddcc177c139"

         },

         {

             "key_ID": "0a782fb5-3434-48fe-aa4d-14f41d46cf92"

         },
}
```

3.3. Error data format

Error data format is used for an error response data model of API "Get status" method, "Get key" method, and "Get key with key IDs" method. JSON data format of Error shall be as follows.

Items	Data type	Description
message	string	Error message
details	array of objects	(Option) Array to supply additional detailed error information specified asname/value pairs. Values may be of any type, including objects.

Examples of Error data format is as follows.

```
{
    "message": "key data access
}



    "message": "not all extension_mandatory parameters are supported","details": [

        {

            "extension_mandatory_unsupported": "abc_route_type is not supported"

        }
}
```

J. SUMMARY OF TEST RESULTS

GR/IR No._____

TSTP No._____

Equipment name & Model No._____

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

[Add as per requirement]

Date:

Place:

Signature & Name of TEC testing Officer /

**** Signature of Applicant / Authorized Signatory***

**** Section J as given above is also to be submitted by the Applicant/ Authorised signatory as part of in-house test results along with Form-A. The Authorised signatory shall be the same as the one for Form 'A'.***

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