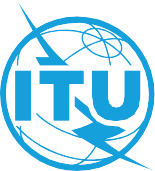
|  |  |  |
| --- | --- | --- |
|  | | Standardization Sector |
| ITU-T Technical Report | |
| (03/2025) | |
|  | **TR.SQKDN** | |
|  | Standardization consideration of satellite-based QKDN | |

|  |  |
| --- | --- |
| **ITUPublications** | **International Telecommunication Union** |



|  |
| --- |
| Technical Report ITU-T TR.SQKDN  Standardization consideration of satellite-based QKDN |

|  |
| --- |
| Summary  Satellite-based quantum key distribution network (QKDN) refers to a secure communication network that employs quantum key distribution (QKD) via satellites to generate and distribute encryption keys.  This Technical Report reviews progress in satellite-based QKDN and related documents of satellite-based QKDN from standards development organizations. The introduction of use cases and general technical information of satellite-based QKDN are discussed. In addition, gap analysis and suggestions on the standardization of satellite-based QKDN are given in this Technical Report for reference purposes. |

|  |
| --- |
| Keywords  Ground station, QKD (quantum key distribution), QKDN (QKD network), satellite-based QKDN. |

Note

This is an informative ITU-T publication. Mandatory provisions, such as those found in ITU-T Recommendations, are outside the scope of this publication. This publication should only be referenced bibliographically in ITU-T Recommendations.

© ITU 2025

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

**Table of Contents**

Page

1 Scope 1

2 References 1

3 Definitions 1

3.1 Terms defined elsewhere 1

3.2 Terms defined in this Technical Report 1

4 Abbreviations and acronyms 1

5 Conventions 2

6 Introduction 2

7 Introduction of satellite-based QKDN 2

7.1 Progress in satellite-based QKDN 3

7.2 Related documents from SDOs 3

7.3 Scenarios for satellite-based QKDN 5

8 Use case and technical overview of satellite-based QKDN 7

8.1 Use case of satellite-based QKDN 8

8.2 General technical information of satellite-based QKDN 11

9 Standardization consideration 14

Bibliography 16

Technical Report ITU-T TR.SQKDN

Standardization consideration of satellite-based QKDN

# 1 Scope

This Technical Report analyses the architecture and functional requirements of a satellite-based quantum key distribution (QKD) network. In particular, the scope of this Technical Report includes:

– Introduction of satellite-based QKDN;

– Use cases and technical overview of satellite-based QKDN;

– Standardization considerations.

# 2 References

[[ITU-T Y.3800](https://handle.itu.int/11.1002/1000/13990)] Recommendation ITU-T Y.3800 (2019), *Overview on networks supporting quantum key distribution.*

[[ITU-T Y.3801](https://handle.itu.int/11.1002/1000/14258)] Recommendation ITU-T Y.3801 (2020), *Functional requirements for quantum key distribution networks.*

[[ITU-T Y.3802](https://handle.itu.int/11.1002/1000/14407)] Recommendation ITU-T Y.3802 (2020), *Quantum key distribution networks – Functional architecture.*

[ITU-T Y-Suppl.80] ITU-T Y-series Recommendations – Supplement 80 (2023), *ITU-T Y.3800-series – Quantum key distribution networks use cases*.

# 3 Definitions

## 3.1 Terms defined elsewhere

This Technical Report uses the following terms defined elsewhere:

**3.1.1 quantum key distribution (QKD)** [b-ETSI GR QKD 007]:Procedure or method for generating and distributing symmetrical cryptographic keys with theoretical information security based on quantum information theory.

**3.1.2 quantum key distribution network (QKDN)** [ITU-T Y.3800]: A network comprised of two or more quantum key distribution (QKD) nodes connected through QKD links.

NOTE – A QKDN allows sharing keys between the QKD nodes by key relay when they are not directly connected by a QKD link.

**3.1.3 quantum key distribution** **node (QKD node)** [ITU-T Y.3800]: A node that contains one or more quantum key distribution (QKD) modules protected against intrusion and attacks by unauthorized parties.

NOTE – A QKD node can contain a key manager (KM).

## 3.2 Terms defined in this Technical Report

None.

# 4 Abbreviations and acronyms

This Technical Report uses the following abbreviations and acronyms:

ATP Acquisition, Tracking and Pointing

GEO Geostationary Earth Orbit

KM Key Manager

LEO Low Earth Orbit

MEO Medium Earth Orbit

QBER Quantum Bit Error Rate

QKD Quantum Key Distribution

QKDN QKD Network

VPN Virtual Private Network

XOR Exclusive OR

# 5 Conventions

None.

# 6 Introduction

Quantum key distribution (QKD) based on the principles of quantum physics uses individual light quanta in quantum superposition states to provide information-theoretically secure key exchange between distant parties. QKD keys are secure and can be used in a variety of industries, including finance, government, energy, and private data transmission and storage. However, the range of QKD has been restricted to a few hundred kilometres due to the channel losses when using optical fibres or terrestrial free space.

The QKD industry is developing rapidly. Satellite-based QKD is a technique that operates over an open-air channel, connecting two telescopes, which also allows senders and receivers to be positioned at various locations without fibre connections, and even enables global quantum communication. Satellite-based QKD technology supports the QKD network (QKDN) in two ways: longer distribution distances and fewer trusted relays. Compared with the inevitable attenuation problem in optical fibre, satellite-based QKD is better suited for the industrial applications of intercontinental long-distance QKD, a significantly lower number of trusted relays are still necessary when using satellite-based QKD technology for QKDNs. To access the QKDN, developers and manufacturers of satellite-based QKD systems need to negotiate a general framework, and architecture, in addition to other considerations. Enterprises in the upstream and downstream of the industry chain, including optical device suppliers, electronic device suppliers, QKDN providers, satellite platform suppliers, etc., can further standardize their products according to recommendations.

This Technical Report analyses the architecture and functional requirements of a satellite-based QKDN. This Technical Report consists in information on the recent progress of satellite-based QKDN, a review of related standards and publications of satellite-based QKDN, an introduction to use cases and application scenarios related to satellite-based QKDN, the outline of the general technical information of satellite-based QKDN and the standardization outlook of satellite-based QKDN.

# 7 Introduction of satellite-based QKDN

A promising solution for QKD on a global scale is to use satellites, which can easily connect two intercontinental locations on Earth. An important advantage of satellite-based free-space quantum communication is that the photon loss due to atmospheric absorption and scattering mostly occurs within the lower ~10 km of the atmosphere, amounting to approximately 3 dB on a clear day. Most of the photon transmission is across a near-vacuum environment, with negligible absorption and decoherence. In addition, the almost non-birefringence of the atmosphere also ensures the stable transmission of quantum states. The diffraction-induced beam loss in free-space channels is roughly proportional to the square of the distance, whereas loss in fibre channels is predominantly caused by absorption and scattering in the fibre medium, scaling exponentially with distance. Therefore, for long-distance communications (typically hundreds to thousands of kilometres), satellite-to-ground free-space channels have advantages over fibre-optic channels in terms of channel loss. Leveraging these advantages, the development of satellite-to-ground free space channel QKD is pivotal for enabling long-distance communication and global deployment.

## 7.1 Progress in satellite-based QKDN

At present, research teams in several countries have undertaken relevant research work. The first quantum science experiment satellite "Micius" was launched in 2016 from China. A series of groundbreaking experiments were conducted, including satellite-to-ground quantum key distribution, ground-to-satellite quantum teleportation, satellite-to-ground entanglement distribution, the establishment of an intercontinental quantum network, satellite-to-ground entanglement-based quantum key distribution, and the development of an integrated space-to-ground quantum communication network. The Jinan-1 nanosatellite from China with real-time QKD technology was launched in 2022. The Centre for Quantum Technologies (CQT) of the National University of Singapore led the development of the Small Photon-Entangling Quantum System (SPEQS), which was successfully launched aboard the 2U Galassia CubeSat, and completed its characteristics testing in space in 2016. They launched the SpooQy-1 satellite in 2019 to demonstrate the experimental verification of the generation and detection of entangled photon pairs. The CAPSAT nanosatellite from the United States was successfully launched to the International Space Station in 2021, carrying a single photon avalanche detector, aiming to study the repair technology of radiation damage to a single photon detector. The National Institute of Information and Communications Technology (NICT) of Japan verified the transmission of satellite-based quantum states by using optical inter-orbit communications engineering test satellite (OICETS) laser communication satellites in 2009. In 2017, NICT used the SOCRATES laser communication satellite to measure the bit error rate of satellite-based quantum state transmission. The TAU-SAT3 satellite from Israel was launched in 2023. In addition, numerous countries and organizations are developing related scientific satellites, including the QEYSSAT quantum satellite program from Canada, the Nanobob satellite from France, the Q3Sat quantum communications satellite project from Austria, the QUBE micro-nano satellite program in Germany, the ROKS micro-nano satellite program and the SPEQTRE micro-nano satellite program in the UK. Several satellite-based QKD systems and services are being developed by the European Space Agency (ESA), SES Techcom S.A, the Austrian Institute of Technology (AIT), the German Aerospace Centre (DLR), the Max Planck Institute for Optics, ID Quantique and Tesat-Spacecom and others. With the increasing involvement of countries, international organizations, and companies in researching and manufacturing satellite-based QKDN, now is an opportune time to establish international standards for satellite-based QKDN.

## 7.2 Related documents from SDOs

Currently, major international and regional standardization organizations, including the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), the International Telecommunication Union (ITU), the Institute of Electrical and Electronic Engineers (IEEE), the European Telecommunications Standards Institute (ETSI), the European Committee for Electrotechnical Standardization (CENELEC), the Internet Research Task Force (IRTF), and the European Association of National Metrology Institutes (EURAMET) have initiated standardization efforts in the field of quantum communication (QC). This section provides an analysis of the transmission channel and a discussion of satellite-based QKDN within the context of existing documents.

The ISO/IEC initiated the first work item on quantum communication in 2019 under JTC1 SC27. Two international standards [b-ISO/IEC 23837-1] [b-ISO/IEC 23837-2] were published in 2023 which focus on the security risks, security requirements, evaluation, and testing methods of QKD. Among them, the QKD system of single-mode fibre is the standardization object for specification. In 2023, PWI 22061 follows the security framework of the ISO/IEC 23837 series and proposes a security analysis for free-space channel and underwater channel. PWI 22061 emphasizes the security analysis of free-space QKD modules and space optical modules, particularly within satellite-based QKDN, while placing less focus on other modules. Additionally, a new Technical Report (TR) examining the impact of different transmission media on security was initiated by ISO/IEC JTC1 SC27 in October 2024.

A new project proposal on the "Architecture of Free-space Quantum Key Distribution" was submitted to JTC3 ahG 4 in August 2024. This proposal focused on QKD utilizing free-space channels, potentially encompassing satellite-based QKD and other methods involving telescopes for transmitting quantum signals through free-space channels. However, the proposal was not approved during the JTC3 general meeting held in October 2024.

Since 2018, ITU-T has initiated more than 40 international standard projects, focusing on the standardization development of quantum networks. The requirements for transmission channels are outlined in application scenarios [ITU-T Y-Suppl.80] and functional architecture [ITU-T Y.3801] [ITU-T Y.3802]. However, these standards address the channel-related content at a relatively basic level, indicating the need for further refinement and additional standards in the future. Furthermore, research documents [b-ITU-T FG QIT4N D2.4] [b-ITU-T FG QIT4N D2.5] specify that ITU will conduct future standardization research on the QKDNs with various channels, which includes integrating QKDNs with satellite networks (e.g., GEO, LEO, inter-satellite, satellite and ground station).

ETSI initiated the industry specification group on quantum key distribution (ISG-QKD) in 2008 and has since conducted comprehensive standardization efforts covering application cases, components, interfaces, security, and terminology. In [b-ETSI GS QKD 002], it clarifies the need to standardize the use case of long-distance QKD service and flying QKD nodes. Subsequent standards primarily focus on QKD systems utilizing optical fibre as the quantum channel. For example, in the [b-ETSI GS QKD 011], Chapter 4.1 claims that the document focuses on the QKD system using fibre. Similarly, the scope defined in the [b-ETSI GS QKD 012], clearly indicates that the QKD system using a fibre optical network is specified in this document. However, analysis or specification for QKD using free space channel are insufficient or absent. To address this gap, a technical specification (TS) for satellite-quantum key distribution (S-QKD) satellite systems & associated optical earth stations (OES) has been proposed in Technical Group: satellite earth stations & systems (SES). This document is under study to focus on use cases, reference architectures, QKD protocols, optical space link transmission characteristics, and technical/operational measures of satellite-based QKD systems, rather than analysis of satellite-based QKDNs. Currently, the work remains in the initial stages, with no relevant draft published yet.

In the standardization roadmap [b-CEN&CENELEC FGQT Q04] published by the CEN&CENELEC Focus group on Quantum Technology, there are currently no contributions to the standardization of QKD using free-space channels, satellite modules, or networks. Given the rapid development of satellite-based QKD, it is essential to initiate standardization efforts in these areas.

In addition, the purpose of the publication by the consultative committee for space data systems (CCSDS) [b-CCSDS 141.0-B-1] is to specify the physical layer characteristics of free-space optical communication systems used by space missions. This standard focuses on the physical layer characteristics of free-space optical communications systems, which use classical optical channels and focus on characteristics. However, in QKDN, satellite-based QKD requires spatial optical modules to establish space quantum channels and adjust parameters. These systems demand additional functional requirements and different characteristic specifications. While CCSDS standards focus on the architecture, protocols, and characteristics of free-space optical communication systems, they are not suitable for free-space satellite satellite-based QKD systems.

In conclusion, the demand of standards for satellite-based QKDN is growing due to its rapid development. However, existing published standards for QKDN or QKD could not overlay the requirements of satellite-based QKD systems, and the current work items under study are insufficient, especially for the modules beyond quantum layers. Therefore, standardization efforts for satellite-based QKD are crucial within ITU-T, along with an analysis of use cases and the current state of the technology.

## 7.3 Scenarios for satellite-based QKDN

The satellite-based QKD system involves ground stations equipped with QKD hardware that communicate with orbiting satellites. These satellites are equipped with QKD modules capable of generating, transmitting, and/or receiving quantum keys. These keys are then employed to encode and decode data, ensuring confidentiality and integrity during transmission. There are multiple scenarios for satellite-based QKD:

Scenario-Ⅰ: Satellite-to-ground QKD

A satellite and satellite dish

AI-generated content may be incorrect.

Figure 1 – Satellite-to-ground QKD

In space-to-ground QKD, the satellite can serve as either the transmitter or the receiver. As a transmitter, the satellite prepares quantum states and transmits them to the ground station, where measurements are taken to generate a shared key. As a receiver, the satellite detects quantum states sent from the ground station, performing measurements to generate a shared key.

NOTE – Quantum states can be transmitted or received using a telescope or a microwave antenna, depending on the specific technical implementation. The figures in this document are provided as examples and do not impose limitations on the technical approach.

Scenario-II: Satellite-based QKD with ground station as relay

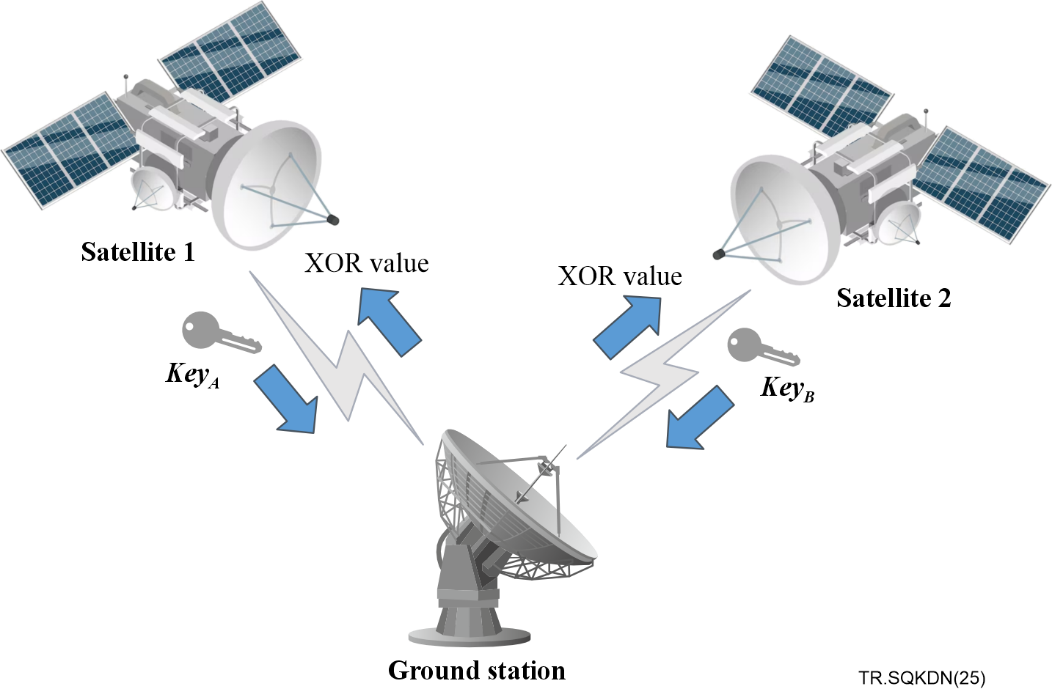


Figure 2 – Satellite-based QKD with ground station as relay

However, it is not easy to load a single photon detector on the satellites. Therefore, the scenario of satellites as the receiver of quantum key distribution is not very realistic. It is possible to use the satellite as the transmitter and the ground station as a receiver, that is, the ground station as a trusted relay between two satellites or between the satellite and space station. In this scenario, satellite 1 and satellite 2 send key A and key B respectively to the ground station, and the ground station returns the XOR value. The two satellites then calculate the shared key. Figure 3 shows trusted repeater based satellite QKD.

Scenario-Ⅲ: Trusted repeater based satellite QKD

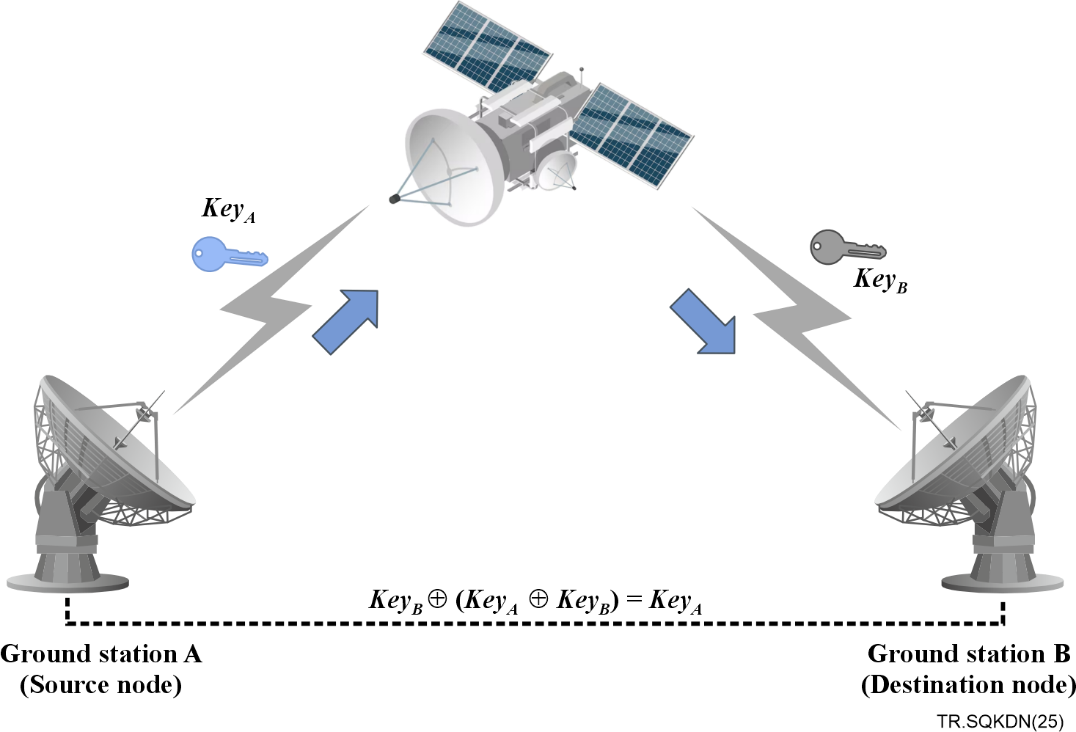


Figure 3 – Trusted repeater based satellite QKD

The satellite engages in QKD processes with different ground stations to create separate secret keys respectively and retains control of entire generated keys, while the individual station only possesses the access to their respective keys. To facilitate the establishment of shared keys between any pair of stations, noted as stations A and B, the satellite aggregates their individual keys and broadcasts the bitwise parity of these keys. By using this broadcasting information from satellites, stations can access each other's keys.

As the original keys are distinct secret sequences, their bitwise parity constitutes a uniformly random string, thus the parity broadcast will not have any valuable data to potential eavesdroppers. Nevertheless, given that the satellite possesses all keys, an adversary gaining access to the satellite's data would attain comprehensive knowledge of the key. Consequently, trust in the satellite is imperative.

Scenario-Ⅳ: Trusted repeater based multi-satellite QKD

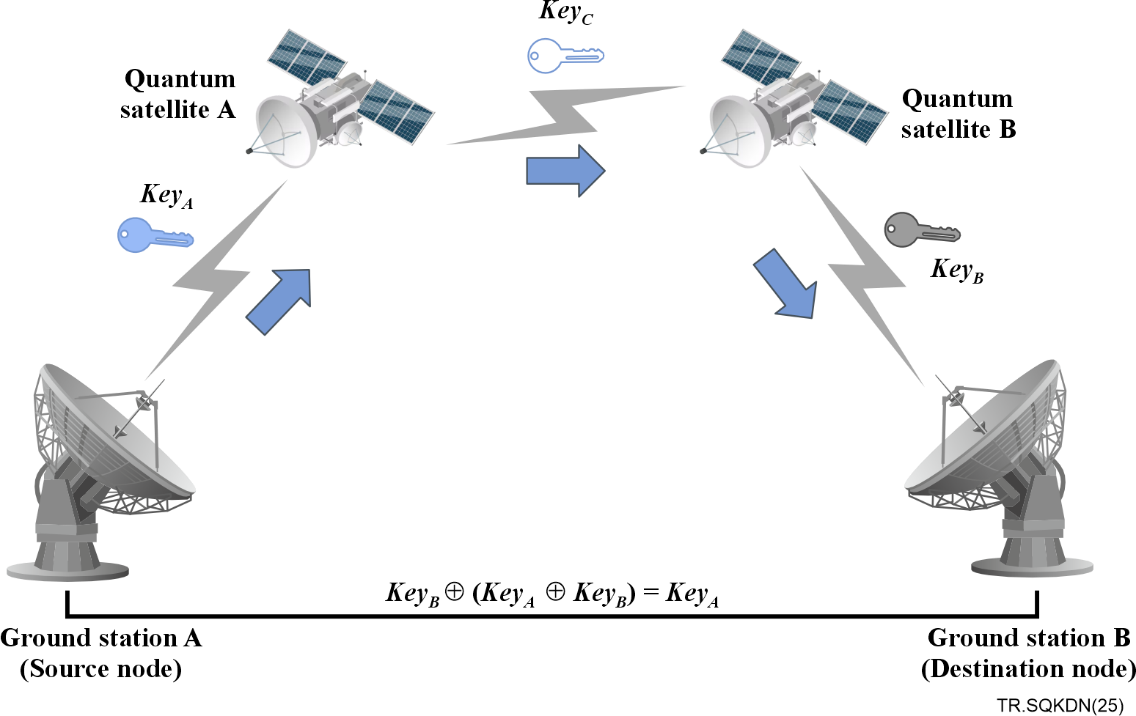


Figure 4 – Trusted repeater based multi-satellite QKD

Two or more quantum satellites can also be used as trusted repeaters in generating secret keys for terrestrial nodes. Similar to terrestrial QKD networks, such satellites can be considered as trusted sources. With a group of such quantum satellites, real-time secret key distribution can be achieved between a pair of ground stations. Figure 4 shows the trusted repeater based QKD through multiple satellites. The secret key can be transmitted from ground station A to ground station B by successively encrypting and decrypting on intermediate nodes. The bitwise parity will be conducted on each link. Considering the long distance between the satellites and the delay in the network, the quantum key pool can be established and utilized within each node.

Furthermore, a combination of inter-layer and intra-layer links can enable more complex satellite-QKD architectures.

# 8 Use case and technical overview of satellite-based QKDN

This clause outlines the use cases of satellite-based QKDN, including ground-to-ground QKDN relay, inter-satellite QKDN, and integrated space-to-ground QKDN. Furthermore, it provides a comprehensive description of the general technical information underpinning these use cases, addressing technical challenges, illustrative implementation examples, and the operational processes involved in satellite-based QKDN.

## 8.1 Use case of satellite-based QKDN

### 8.1.1 Trusted relay node of long-distance ground-to-ground QKDN

#### 8.1.1.1 Transnational business

Nowadays, international cooperation and exchanges are constantly strengthened, and cross-border business projects are increasing. There is a growing demand for data transmission, audio and video meetings and data supervision needs between overseas branches and domestic headquarters.

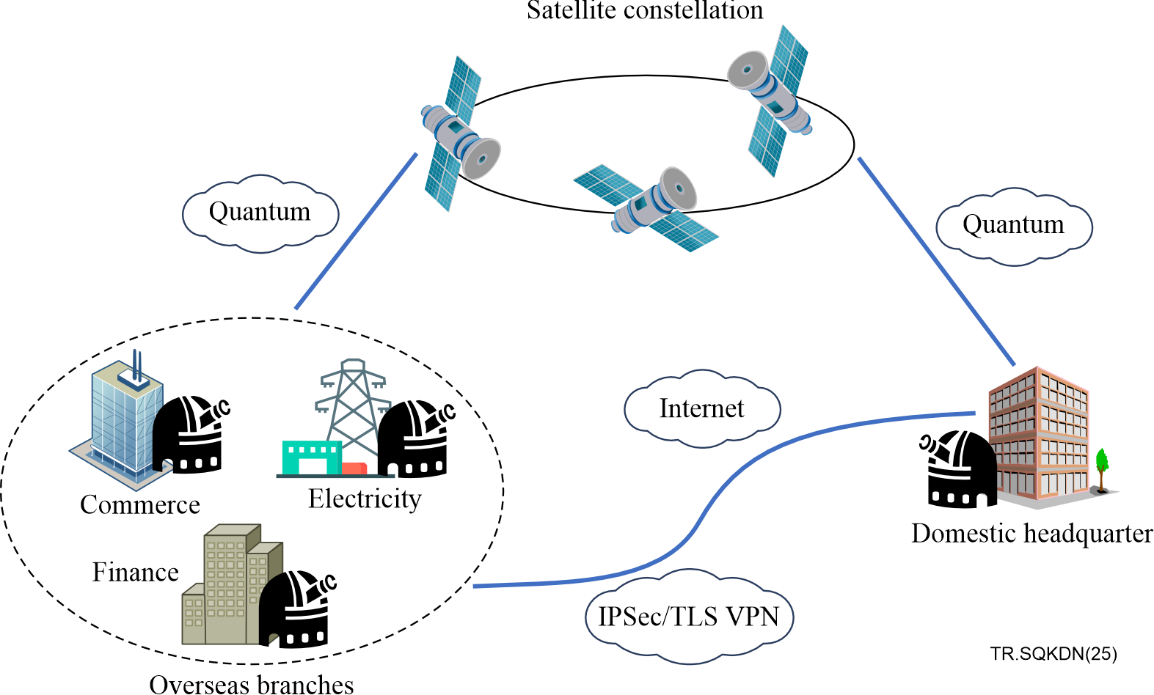


Figure 5 – Cross-border business

As shown in Figure 5, for international business, enterprises and institutions typically employ a combination of the Internet and dedicated information security equipment to protect their information systems, such as Internet protocol security (IPSec) VPN or transport layer security (TLS) VPN technology. The utilization of quantum satellites and ground stations enables the global distribution or transfer of keys for these network layers or link layers in the encryption devices and key management systems, meeting the data encryption needs of enterprises and institutions operating overseas, thereby enhancing the data security of international operations.

The communication security between overseas branches and domestic headquarters of enterprises and public institutions is effectively safeguarded by the global, wide-area QKD via satellites.

#### 8.1.1.2 Mobile service business

In certain specialized environments, secure communication is required while the user remains in continuous motion. During maritime operations, ships need to maintain secure communication with headquarters while in transit. By employing satellite relays, QKD can be achieved between ship-based ground stations and fixed stations. The key distribution and relay services between regional quantum communication ground stations can also be realized, as illustrated in Figure 6.

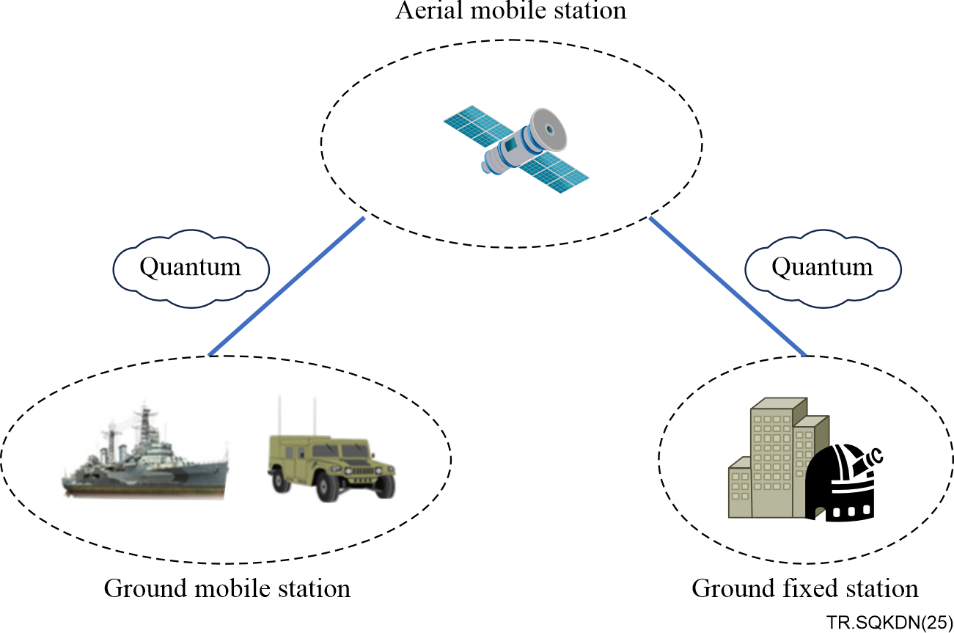


Figure 6 – Mobile service business

In use cases requiring continuous mobility, long-distance and wide-area QKD services are provided to user groups with special needs through the deployment of satellites.

#### 8.1.1.3 Connecting to the ground fibre quantum network

Another viable use case involves connecting remote nodes to the quantum communication backbone network through satellite-based QKD. For instance, China has established ground-based optical fibre quantum metropolitan area networks and backbone networks in various regions, including the Beijing-Shanghai Trunk Line for quantum secure communication, which links metropolitan networks in Beijing, Jinan, Hefei, Shanghai, and other cities. Nevertheless, the ground-based backbone network has not yet been extended to the western regions, and metropolitan networks in Hainan, Chengdu, Urumqi, and other places areas currently lack connectivity with the eastern coastal regions.

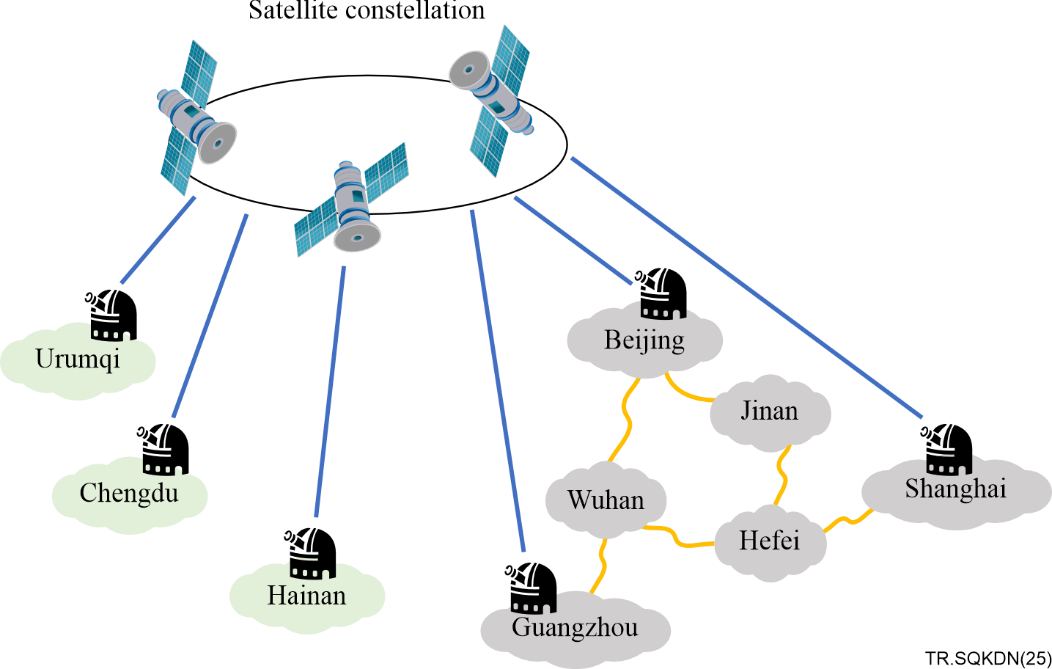


Figure 7 – Connecting to the ground fibre quantum network

As illustrated in Figure 7, to facilitate the deployment of quantum communication ground stations in the aforementioned cities and establish connectivity with the metropolitan networks, cross-domain connections can be realized via quantum communication satellites. This approach enables users currently connected to the metropolitan networks to access wide-area quantum secure communication services.

### 8.1.2 Realization of inter-satellite QKDN

A single-layer satellite-based simple QKDN is robust and resilient and produces a limited number of secure keys, which may be insufficient for applications demanding higher levels of security. As global services continue to expand, the demand for confidentiality and secure information transmission is becoming increasingly critical. Whether for communication between nations or commercial organizations, relying solely on ground-based stations makes it challenging to achieve end-to-end QKD on a global scale. Given the inherent physical constraints of QKD and the pressing need for enhanced communication security due to the rising risk of attacks on space networks, satellite-based solutions are essential for enabling end-to-end QKD worldwide.

A high-security general-purpose long-haul network utilizing multi-layer satellite architecture on a global scale has been proposed [b-ITU-T FG QIT4N D2.2]. By employing multi-layer satellites as relays, long-range QKD can be effectively achieved across major metropolitan areas worldwide.

As illustrated in Figure 8, the general-purpose long-haul network based on a multi-layer satellite system comprises three tiers: geostationary earth orbit (GEO) satellite, medium earth orbit (MEO) satellite, and low earth orbit (LEO) satellite. This multi-layer satellite architecture in orbit serves as an essential component of a general-purpose long-haul network, which enables worldwide coverage through satellite communication, providing flexible access for users. The global QKDN architecture leveraging the multi-layer satellite network is established, and the nodes are interconnected via not only satellite-to-ground links but also inter-satellite links, ensuring seamless connectivity.

Each GEO satellite is tasked with key management and distribution within its designated coverage areas while the LEO and MEO satellites function as QKDN transmitter and receiver terminals. The ground control node oversees unified key management and distribution across the entire general-purpose long-haul network, encompassing both satellite and terrestrial networks.

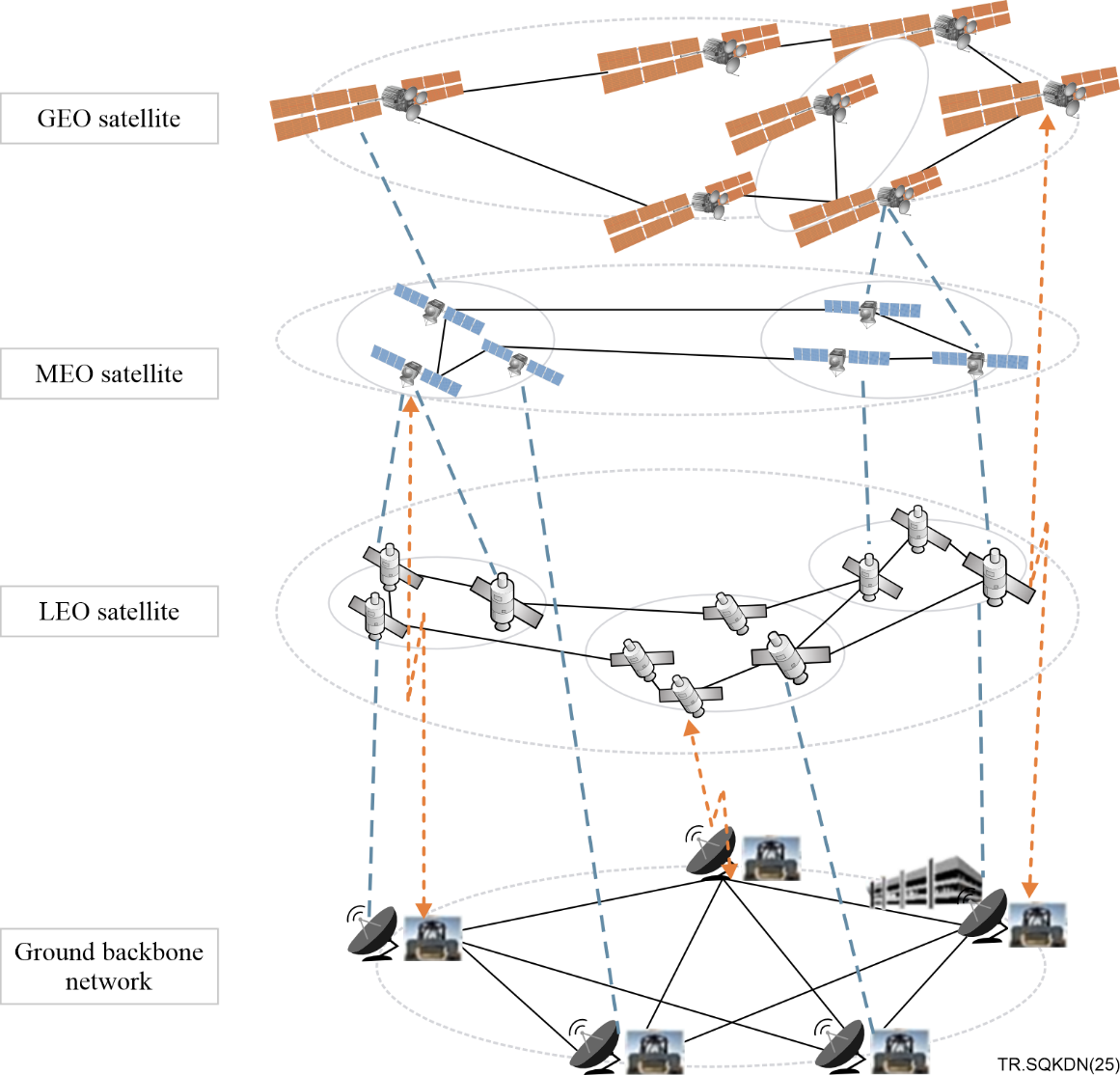


Figure 8 – General-purpose long-haul network based on multi-layer   
satellite QKD [b-ITU-T FG QIT4N D2.2]

This technology is particularly well-suited for remote regions where the high cost of deploying optical fibre presents a significant barrier to implementing QKD. Moreover, it effectively addresses the challenges associated with providing secure communication for mobile users in hard-to-reach locations, such as maritime mobile platforms, polar research stations, and desert monitoring stations.

At the same time, a systematic study on the standardization of integrating QKDN into satellite networks is necessary. This study should encompass architectural implications, technical requirements for satellites and ground stations, as well as protocols, performance, and security specifications.

## 8.2 General technical information of satellite-based QKDN

This clause will introduce technical challenges in satellite-based QKDN, the implementation of the satellite-based QKD, and the working flow of space quantum secure communication networks based on satellites.

### 8.2.1 Technical challenges in satellite-based QKDN

In the process of implementation, satellite-based QKDN faces some technical challenges due to its unique characteristics:

– In satellite-based QKD, it is crucial to address technical challenges, such as signal degradation and environmental interference. In addition to sunlight, local weather conditions, and other atmospheric losses, cloud cover can affect QKD transmission. Advanced error correction and classical post-processing techniques and adaptive optics play a vital role in maintaining the fidelity of quantum communication links.

– In long-distance QKD implementation, in which polarization of light is commonly used, a degree of freedom is becoming increasingly important. However, there is a significant challenge from photon-polarization getting affected due to the birefringence of fibres in fibre-based implementations, or variation of reference frames due to satellite movement in long-haul demonstrations. Conventionally, active feedback-based mechanisms are employed for real-time polarization tracking. The conventional active feedback system-based polarization tracking techniques are resource-intensive, resulting in additional maintenance costs. A polarization-based compensation method that obviates the need for active polarization tracking in satellite-based QKD implementations is proposed in [b-Chatterjee]. It serves as an effective tool towards enabling efficient long-range QKD implementations for both fibre-based and free-space approaches.

– Time synchronization among the geographically distributed nodes and phase stabilization (depending on the protocol) is important for satellite-based QKD.

– Satellite-based QKDN faces security threats, particularly arising from the reliance on free-space optical channels, protocol-specific weaknesses, and device-specific vulnerabilities, when there is no proper protection. These additional components are unique to satellite-based QKD systems, probably introducing new security risks.

### 8.2.2 Implementation of satellite-based QKD

Scenario-Ⅰ introduced in clause 7.3 is used as an example to illustrate the implementation of satellite-based QKD. A complete satellite-based QKD system consists of a satellite platform which contains a QKD load, a ground station which contains OKD and optical modules, and a control system which is responsible for the whole process management and coordination of QKD, see Figure 9. The acquisition, tracking and pointing (ATP) systems in the QKD load and optical module establish a quantum optical link between the satellite platform and ground station through mutual acquisition, tracking and pointing. The quantum light source in the QKD transmitter of the satellite platform generates the quantum signal and the synchronous signal, which are transmitted through the quantum channel in free space via the ATP system, and are received by the ATP system of a ground station. The QKD receiver in the ground station detects the received quantum signal and synchronous signal. After accumulating enough data, the two communication parties use the classical channel to negotiate the key and ultimately generate the quantum key.

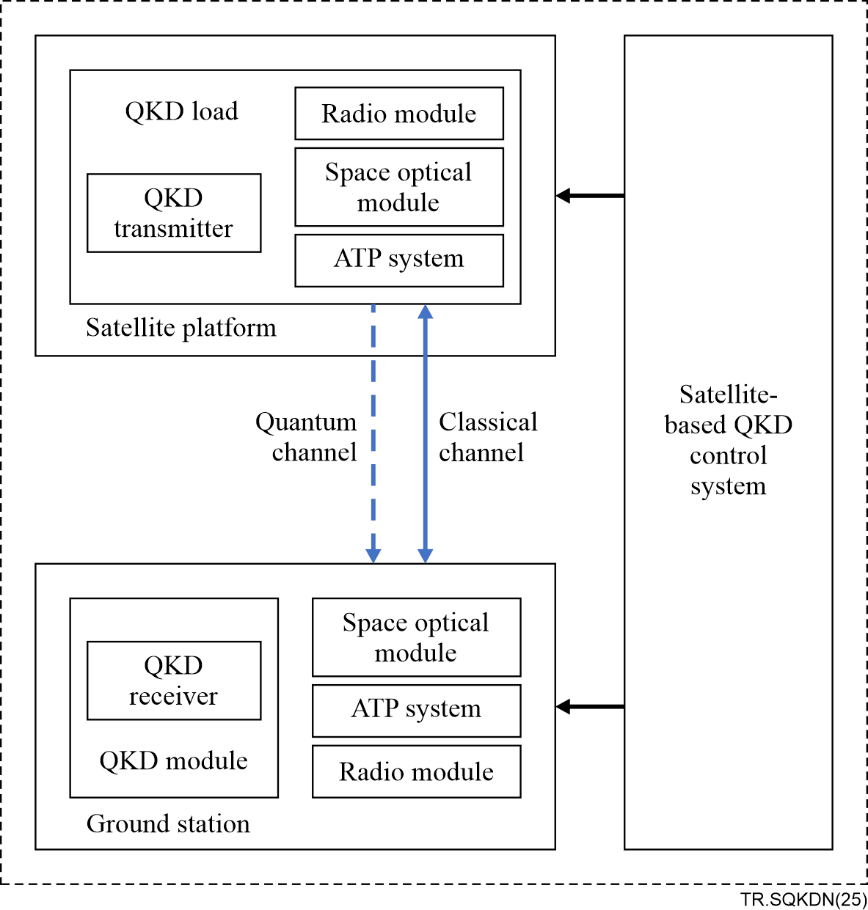


Figure 9 – Components of satellite-based QKD system

The quantum channel in satellite-based QKD consists of the atmosphere or vacuum. Unlike the fixed attenuation characteristic of optical fibres, photon transmission through the atmosphere is primarily influenced by factors such as atmospheric absorption, scattering, turbulence, refraction, and beam divergence.

The space optical module is a critical component of the beam transmitting and receiving in the terminal of the satellite-based QKD. To facilitate QKD, the transceiver terminal needs to establish a precise and stable optical link. Given the importance of link efficiency in the satellite-based QKD, the divergence angle of the quantum signal is generally designed to approach the diffraction limit. On the receiver side, the space optical module reduces the beam aperture and provides a collimated beam with high image quality for the beam-splitting system. On the transmitter side, its function is to expand the beam aperture and decrease the divergence angle of the emitted beam.

In order to direct the very narrow quantum light signal from the transmitter to the receiver, it is necessary to use beacon light to aid in establishing the optical link. This process is typically divided into three steps: acquisition, tracking and pointing (ATP). Acquisition refers to the process of locating one side of the communication link relative to the other. Tracking involves both parties controlling tracking mechanisms based on the deviation of the optic axis provided by the detector, ensuring that the receiving optical axis follows the changes of the transmitting optical axis. Finally, based on the tracking process, pointing refers to the precise alignment of the optical axes of both parties, ensuring that their respective lines of sight are correctly aimed at each other's positions.

The classical channel utilized for transmitting key negotiation information can be implemented using laser communication via space optical modules or telecommunication through radio modules.

### 8.2.3 Working flow of satellite-based QKD

The satellite-based QKD enables key collaboration across vast areas. In particular, satellite-based QKD can achieve global coverage, establish a space-to-ground quantum secure communication network, and connect remote locations such as overseas regions, distant reefs, vehicles, ships, and areas not currently served by terrestrial fibre networks.

In satellite-based QKDN, satellites, ground stations, and network controllers primarily utilize free-space channels to facilitate the exchange of quantum signals and classical data.

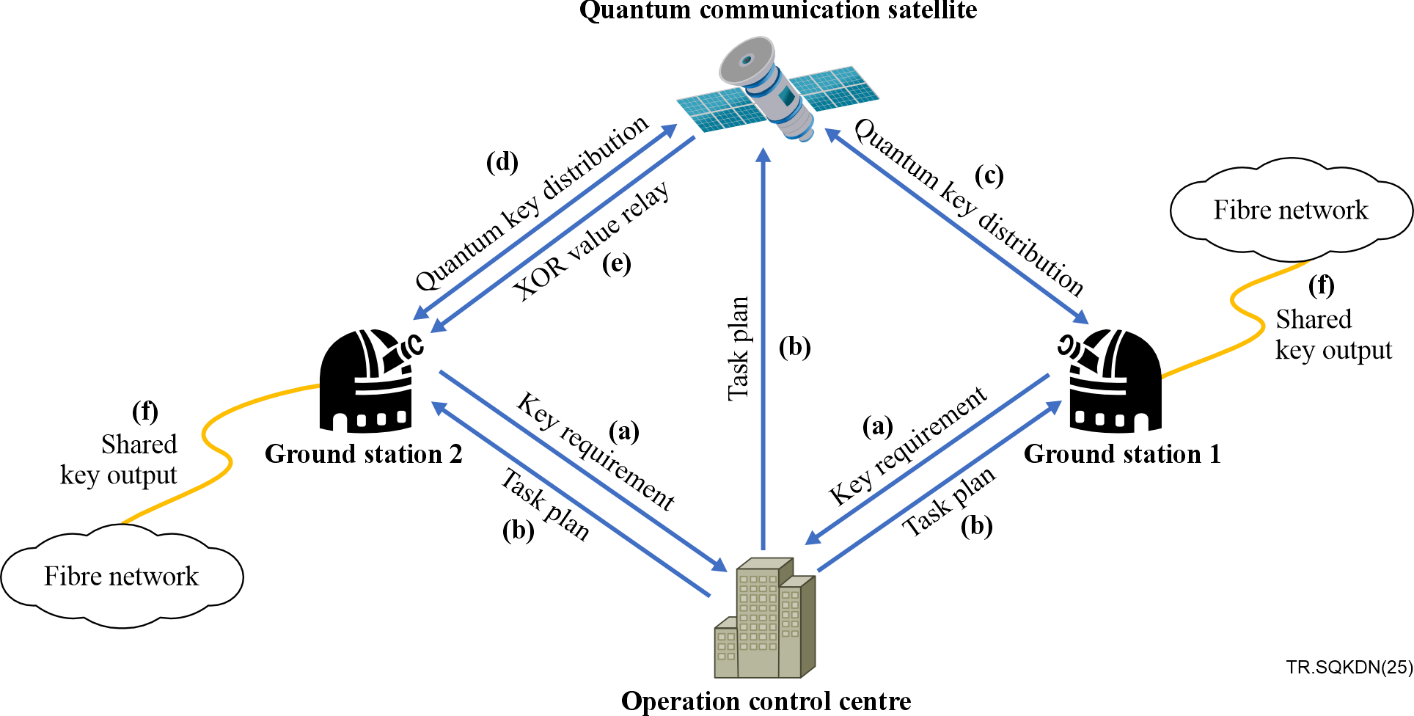


Figure 10 – Working flow of satellite-based QKD

Figure 10 illustrates the main flow of a typical satellite-based QKD process:

a) The ground station sends the key requirements to the operation control centre based on the user's needs.

b) The operation control centre develops a task instruction plan, sends the instructions to the satellite through the measurement and control station, and sends the mission plan to the ground station.

c) The quantum communication satellite and ground station 1 dock at the scheduled time to begin the satellite-ground docking task and complete quantum key distribution.

d) The quantum communication satellite and ground station 2 dock at the scheduled time to begin the satellite-ground docking task and complete quantum key distribution

e) The quantum communication satellite sends the XOR value of the keys of the two ground stations to the second ground station to complete the key relay.

f) The two ground stations respectively output the paired quantum key to the ground fibre network, which then relays the key to the user node.

# 9 Standardization consideration

Satellite-based QKDN remains an evolving technology. Challenges surrounding the standardization of satellite-based QKDN span a wide range of areas, from use cases to communication networks, and security concerns. Future efforts in satellite-based QKDN standardization may address aspects that could potentially resolve the issues outlined below:

Application scenarios and use cases

In addition to ground-to-ground long-distance QKDN, inter-satellite QKDN, and integrated space-to-ground QKD networks, further research and exploration of additional application scenarios are necessary. This need is driven by technological advancements in satellite-based QKD and QKDN, as well as emerging and specific applications.

Network architecture

The development of an integrated space-to-ground quantum-secure communication network is essential for achieving global QKD coverage. Satellite-based QKDN plays a vital role in this global network. Standardization of satellite-based QKDN needs to address key aspects of network construction and operation, including architecture, interfaces, node deployment strategies, and interconnectivity specifications.

Integration with existing communication networks

Satellite-based QKDN needs to be designed to integrate with existing fibre-based QKD networks, classical optical communication networks, wireless communication systems, and satellite communication infrastructures. Standardization needs to focus on key aspects such as quantum-classical channel multiplexing, protocols and interfaces between different networks, and mechanisms for interoperability.

Technical implementation and QoS

The functions and performance necessary for the implementation and quality of service of satellite-based QKDN may be standardized. This includes key parameters such as quantum bit error rate (QBER), key generation rate, synchronization accuracy, and channel stability under varying atmospheric and environmental conditions. These standards also provide guidance for the testing and evaluation of satellite-based QKDN, which is essential for users.

Security

Satellite-based QKDN integrates additional components, such as the ATP system and space optical modules, and operates in outer space, where it is remotely controlled under challenging environmental conditions. These factors may introduce security challenges that are not present in fibre-based QKDNs. Therefore, conducting risk analysis and establishing standardized security functions, testing methods, and evaluation criteria are essential to ensuring the certifiable security of satellite-based QKDN.

Bibliography

[b-ITU-T FG QIT4N D2.2] Technical Report FG QIT4N D2.2 (2021), *Use cases: Quantum key distribution network*.

[b-ITU-T FG QIT4N D2.4] Technical Report FG QIT4N D2.4 (2021), *Quantum key distribution network transport technologies*.

[b-ITU-T FG QIT4N D2.5] Technical Report FG QIT4N D2.5 (2021), *Standardization outlook and technology maturity: Quantum key distribution network*.

[b-Chatterjee] Chatterjee, Sourav, *et al.* (2023), *Polarization bases compensation towards advantages in satellite-based QKD without active feedback*. Communications Physics 6.1: 116.

[b-CCSDS 141.0-B-1] Recommended Standard CCSDS 141.0-B-1 (2019), *Optical communications physical layer*.

[b-CEN&CENELEC FGQT Q04] CEN&CENELEC Focus Group on Quantum Technologies FGQT Q04 (2023), *Standardization Roadmap on Quantum Technologies*.

[b-ETSI GS QKD 002] Group Specification ETSI GS QKD 002 (2018), *Quantum Key Distribution (QKD); Use Cases*.

[b-ETSI GR QKD 007] ETSI GR QKD 007 V1.1.1 (2018), *Quantum Key Distribution (QKD); Vocabulary*.

[b-ETSI GS QKD 011] Group Specification ETSI GS QKD 0011 (2016), *Quantum Key Distribution (QKD); Component characterization: characterizing optical components for QKD systems*.

[b-ETSI GS QKD 012] Group Specification ETSI GS QKD 0012 (2019), *Quantum Key Distribution (QKD); Device and Communication Channel Parameters for QKD Deployment*.

[b-ISO/IEC 23837-1] International Standard ISO/IEC 23837-1 (2023), *Information security – Security requirements, test and evaluation methods for quantum key distribution; Part 1: Requirements*.

[b-ISO/IEC 23837-2] International Standard ISO/IEC 23837-2 (2023), *Information security – Security requirements, test and evaluation methods for quantum key distribution; Part 2: Evaluation and testing methods*.

[b-Xu] Xu, Minrui, *et al.* (2022), *Quantum-secured space-air-ground integrated networks: Concept, framework, and case study*. IEEE Wireless Communications 30.6: 136-143.

\_\_\_\_\_\_\_\_\_\_\_