Work Progress on Quantum Key Distribution Network Use Cases in ITU-T FG-QIT4N

Zhangchao Ma

CAS Quantum Network Co., Ltd.

FG-QIT4N WG2 Chair

10 June 2020

Setting the standard

FG-QIT4N activities on QKDN use cases

D2.1	Technical report on QIT4N terminology part 2: quantum key distribution network
D2.2	**Technical report on the QIT4N use case part 2: quantum key distribution network**
D2.3	Technical report on QKDN protocols
D2.4	Technical report on QKDN transport technologies
D2.5	Technical report on QIT4N standardization outlook and technology maturity part 2: quantum key distribution network

D2.2 Leadership

Leader & Chief editor: Mr. Andreas Poppe (AIT, Austria)
Co-editors:

- Mr. Thomas Laenger (AIT, Austria)
- Mr. Dong-Hi Sim (SKT, Korea, (Rep. of))
- Mr. Zhangchao Ma (CAS Quantum Network Co., Ltd., China)

1st FG-QIT4N meeting
- 9 - 10 December 2019, Jinan, China
- 7 input contributions on QKDN
- Deliverables structure agreed

2st FG-QIT4N meeting
- 18-20 February 2020, e-meeting
- 13 inputs on QKDN, 4 on use cases
- D2.2 initial skeleton agreed w template for soliciting use case

3st FG-QIT4N meeting
- 20-30 April 2020, e-meeting
- 22 inputs on QKDN, 6 on use cases
- Six use cases captured

4st FG-QIT4N meeting
- 15-26 June 2020, e-meeting
- Joint session with ETSI ISG QKD

5st FG-QIT4N meeting
- August 2020, TBD

……

Setting the standard

D2.2 Technical report on the QIT4N use case part 2: quantum key distribution network

Summary

This document consolidates the real-world QKDN use cases gathered during the lifetime of the ITU-T Focus Group on Quantum Information Technology for Networks (FG QIT4N).

The QKDN uses cases are classified into vertical and horizontal domains. And it also highlights the competitive advantage of use cases brought by QKDN, the main barriers to QKDN adoption, and the benefits and needs for future standardization efforts.

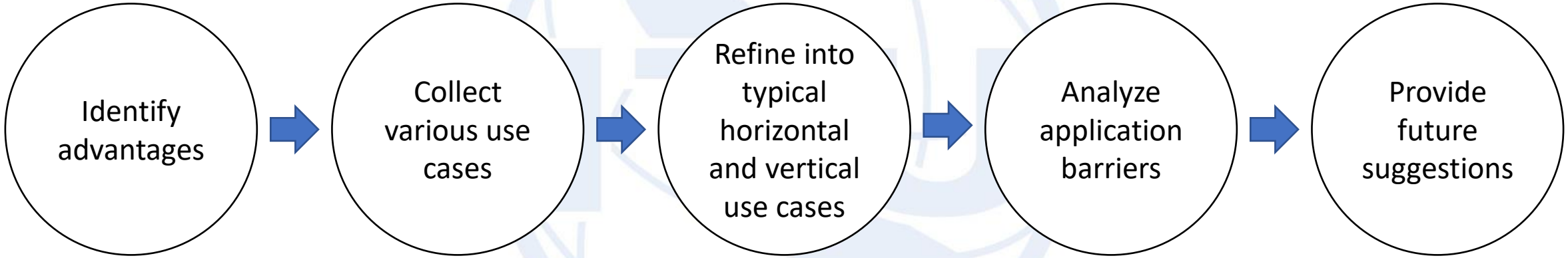
Scope

- Competitive advantage brought by QKDN
- QKDN use cases in vertical and horizontal domains
- Barriers for QKDN adoption
- Suggestions for future works

Table of Contents

Latest version: QIT4N-O-024

Envisioned working stages



Current stage

The competitive advantages of using QKDN

Overview

- to realize secure symmetric key agreement based on the transmission and processing of quantum states
- any eavesdropping behavior will be discovered in time due to the disturbance of the quantum state
- information theoretical security protocol, security not affected by the computing power of the adversary
- need to be combined with conventional cryptography, e.g., QKD+OTP+Universal-2 Hash
- can be integrated with various existing TCP/IP protocols at different layers, e.g., IPSEC, TLS.

Identified benefits

- **QKDN vs. computation complexity based cryptography:** long term security, anti-eavesdropping, quantum computing resistance
- **QKDN vs. symmetric cryptography based key exchange:** perfect forward security
- **QKDN vs. asymmetric cryptography based key exchange (including PQC):** high performance
- To be supplemented…

QKDN use cases collected (draft):
UC-V-010 General purpose high security metropolitan area network

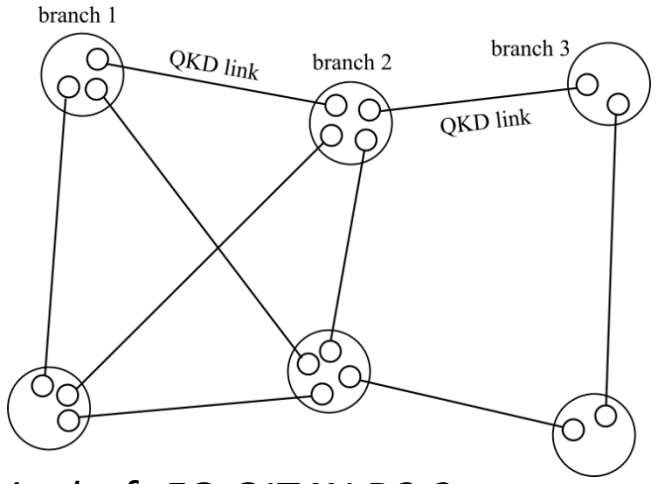
Contributed by: Thomas Länger (AIT)

Target end users:

Administrations, corporations, and other organizations with branches in a metropolitan area, looking for a high security communications network solution.

Scenario:

A general-purpose high security communications network between several branches and offices within an area of about 100km in diameter (metropolitan area). The single network nodes are interconnected with dedicated optical point to point links for classical digital communication and quantum key distribution.



Advantages:

End users can rely on the security of their proper network infrastructures.

They produce their cryptographic secrets with the high security standards of QKD.

End users can select the cryptographic security of their communication and authentication primitives according to their needs.

** Hereby just show selected parts of given use case, see the full description in draft FG-QIT4N D2.2*

QKDN use cases collected (draft):
UC-V-020 Secure cloud archive

Contributed by: Thomas Länger (AIT)

Target end users:

Individuals and organizations looking for an improved storage solution in the cloud with advanced security and privacy guarantees.

Scenario:

Use a cloud archive with advanced privacy and security guarantees, based on a secret sharing primitive, and secure the data links to the single storage providers with QKD links.

Advantages:

The use case counters some of the most severe threats in current cloud solutions and provides a distributed cloud archive with advanced data availability, as well as provable long term confidentiality and integrity guarantees.

The secret sharing primitive exhibits perfect secrecy, i.e. the observation of a number of shares less than the selected threshold provides exact zero information about the plaintext.

The transport of the shares from the end user to the storage providers is secured with the perfect secrecy of onetime pad (OTP) encryption, using ε-secure keys from a QKD link.

** Hereby just show selected parts of given use case, see the full description in draft FG-QIT4N D2.2*

QKDN use cases collected (draft):
UC-V-030 Satellite-based QKD network

Contributed by: Beijing University of Posts and Telecommunications, China; CAS Quantum Network Co., Ltd, China; Ministry of Industry and Information Technology (MIIT), China

Target end users:

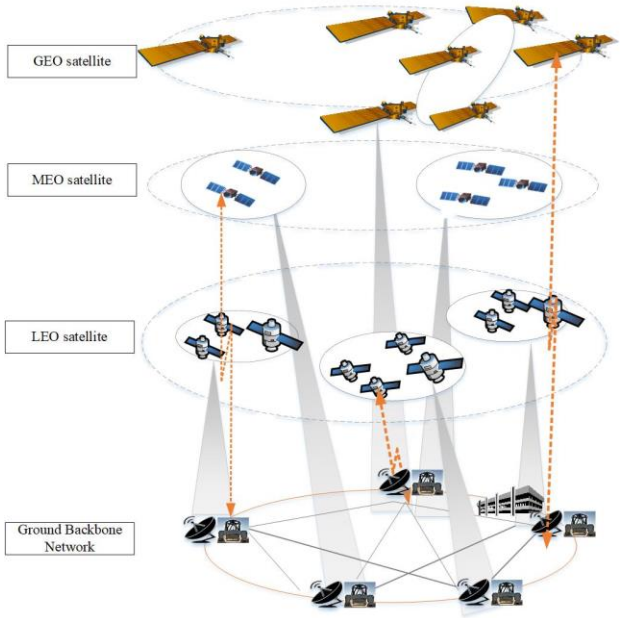
Governments and organizations, especially those end users who can't connect to optical fiber (such as Arctic Research Station), and those with strong mobility (such as naval ships), looking for a high security network solution for connecting different metropolises worldwide

Scenario:
This use case describes a high security satellite-based QKD network around the world. By using satellite as relay, long-distance QKD can be realized within the global metropolises.

Advantages:

Satellite-based QKD network uses satellites as relays, which can achieve end-to-end QKD between two cities worldwide, and greatly enhances timeliness.

Satellite-based QKD network provides wider and denser coverage, and makes it easier for mobile and remote user terminals to use quantum encryption services.



** Hereby just show selected parts of given use case, see the full description in draft FG-QIT4N D2.2*

QKDN use cases collected (draft):
UC-H-010 QKD-equipped SCION architecture

Contributed by: Mingeun Yoon (SK Telecom) and Jonghoon Kwon (ETH Zürich)

Target end users:

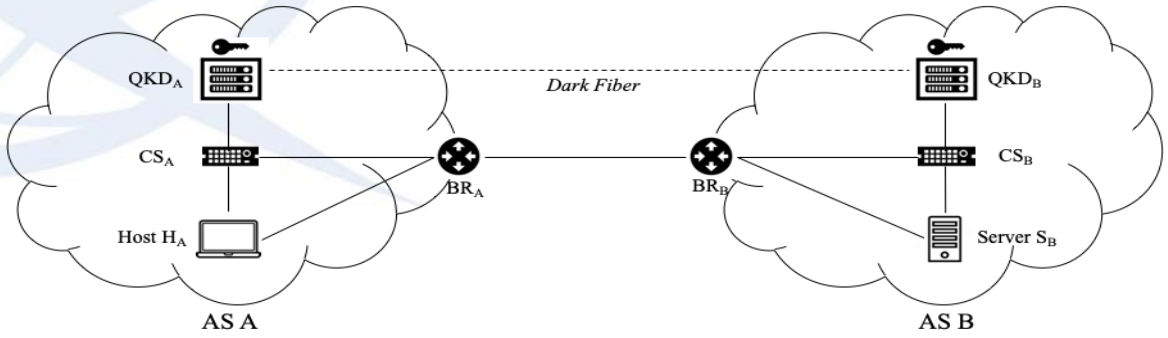
QKD can play an important role in a new internet architecture for enhancing the security which is one of main the concern that today's internet is facing.

Scenario:

SCION (Scalability, Control, and Isolation On Next-Generation Networks) is a proposed Future Internet architecture that aims to offer high availability and efficient point-to-point packet delivery, even in the presence of malicious adversaries and devices by discovering attacker-free path between endpoints.

In SCION architecture, local secret keys are critical since all the end-to-end symmetric keys are derived from them and used in many cases such as control message authentication, source authentication and on-path verification.

By using the keys acquired from QKD as the local key in the integrated architecture, security enhancement can be achieved..



** Hereby just show selected parts of given use case, see the full description in draft FG-QIT4N D2.2*

QKDN use cases collected (draft):
UC-H-020 QKD-key embedded secure mobile communication

Contributed by: Zhangchao Ma (CAS Quantum Network Co., Ltd.)

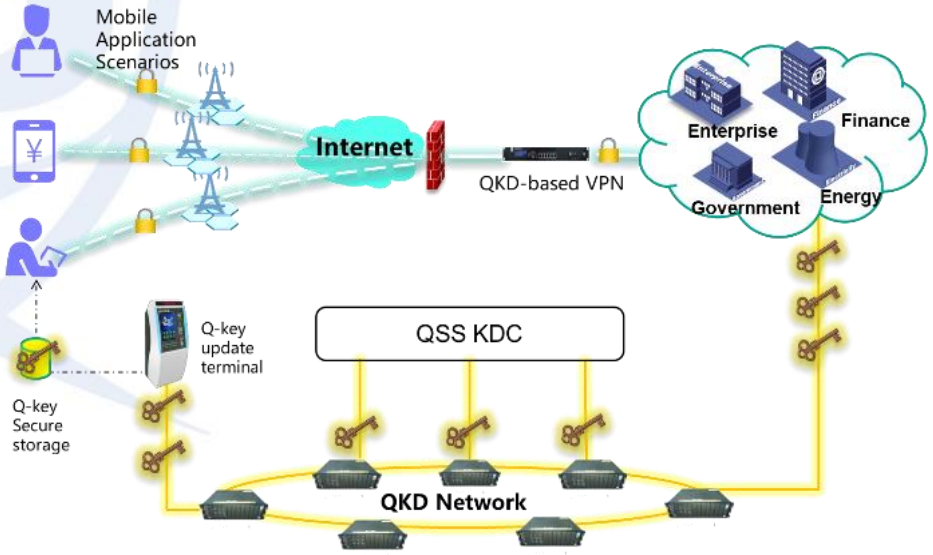
Target end users:

This use case can be applied in many more vertical sector scenarios, e.g., mobile working, mobile payment, industry internet of things.

Scenario:

The solution is to pre-install the QKD-key pool into the mobile user and network side to enhance security of mobile communication which is achievable with existing QKD techniques.

The Q-key update terminal is introduced to cache QKD-key pool and implant the QKD-keys to mobile user equipment (which contain certain secure storage to store the keys). And the KDC at the QKD network side is introduced to store the symmetric key pools and perform key management. The mobile terminals embedded with QKD-key pool can consume the keys provided by QKDN to performs secure communication and recharge QKD-keys from the QKDN once exhausted.



** Hereby just show selected parts of given use case, see the full description in draft FG-QIT4N D2.2*

QKDN use cases collected (draft): UC-H-030 Multi-domain QKDN

Contributed by: Beijing University of Posts and Telecommunications, China; CAS Quantum Network Co., Ltd, China; Ministry of Industry and Information Technology (MIIT), China

Target end users:

The class of VUCs with the characteristic of multiple domains.

Scenario:

As the QKDN deployment extends to the large scale networks, the most realistic QKDN scenario in the future refers to multi-domain scenario. The multiple heterogeneous domains of QKDN are implemented by multiple different vendors and with different technologies, not only due to the diverse data transmission and QKD technologies, but also due to the different options of QKDN control layer techniques. It is necessary to focus on how to ensure the stable and efficient operations of multi-domain QKDN.

In the architecture of multi-domain QKDN, the global multiple-domain QKDN controller serves as a core orchestration player with global view of the whole multi-domain QKDN. The collaboration between the QKDNs in multiple domains under the control of global multiple-domain QKDN controller is necessary to meet the service requirements.

** Hereby just show selected parts of given use case, see the full description in draft FG-QIT4N D2.2*

Call for contributions on QKDN use cases

Plenty of use cases observed but contributions still few:

- ✓ **from industry players**, e.g, ID Quantique, Qubittek, QuantumCTek, …
- ✓ **from testbed & demonstrations**, e.g., OpenQKD, Tokyo QKD, Beijing-Shanghai QKD backbone…
- ✓ **Potential new areas:**
  - ➢ QKD + 5G
  - ➢ QKD + blockchain
  - ➢ QKD + Industrial TSN
  - ➢ …

ITU-T FG-QIT4N:

- ✓ **Open to all**
- ✓ **Free participation:**
  - ➢ **no membership requirement**
  - ➢ **no cost**
- ✓ **Documents publicly available at no cost**

Cooperation and Collaboration to Flourish QKDN Industry!