Introduction of Quantum-secured Communication Standardization in CCSA

Zhangchao Ma

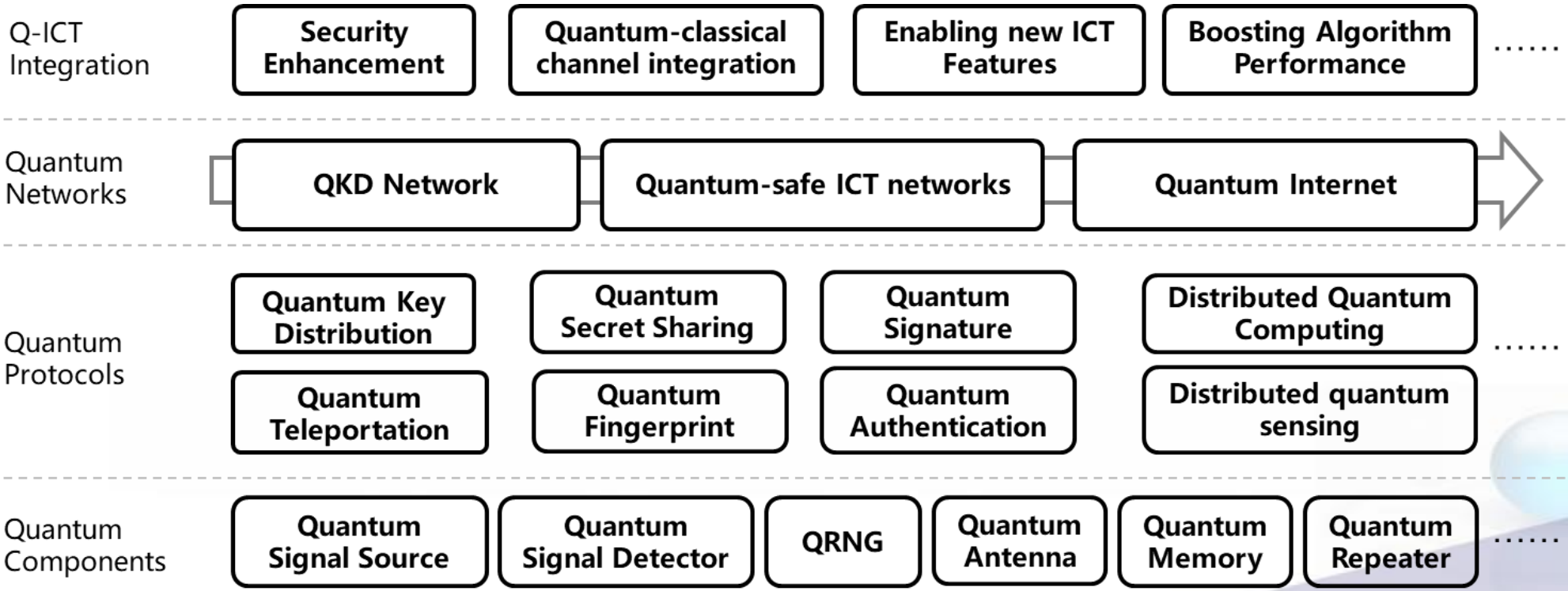
CAS Quantum Network, Co., Ltd.

ST7: Quantum Communication and Information Technology

June 2019

Standardization is key to accelerate QIT industrialization

- **Ensure multi-layer, multi-vendor inter-operability and conformance**
- **Enable scalable deployment and flexible application**
- **Stimulate supply chains of quantum components**



CCSA standardization activity on quantum technology

- In June 2017, CCSA established the 7th Special Task Group (ST7) on Quantum Communication and Information Technology
- ~50 members including QKD & Telecom. network operators, QKD vendors, Telecom. vendors, end users，universities and research institutes.
- Currently focused on quantum-secured communication (QSC) based on QKD and QRNG

Key issues to be standardized for QSC

Application

- Clarify use cases and requirements
- Provide APIs to facilitate easy and flexible applications of QKD

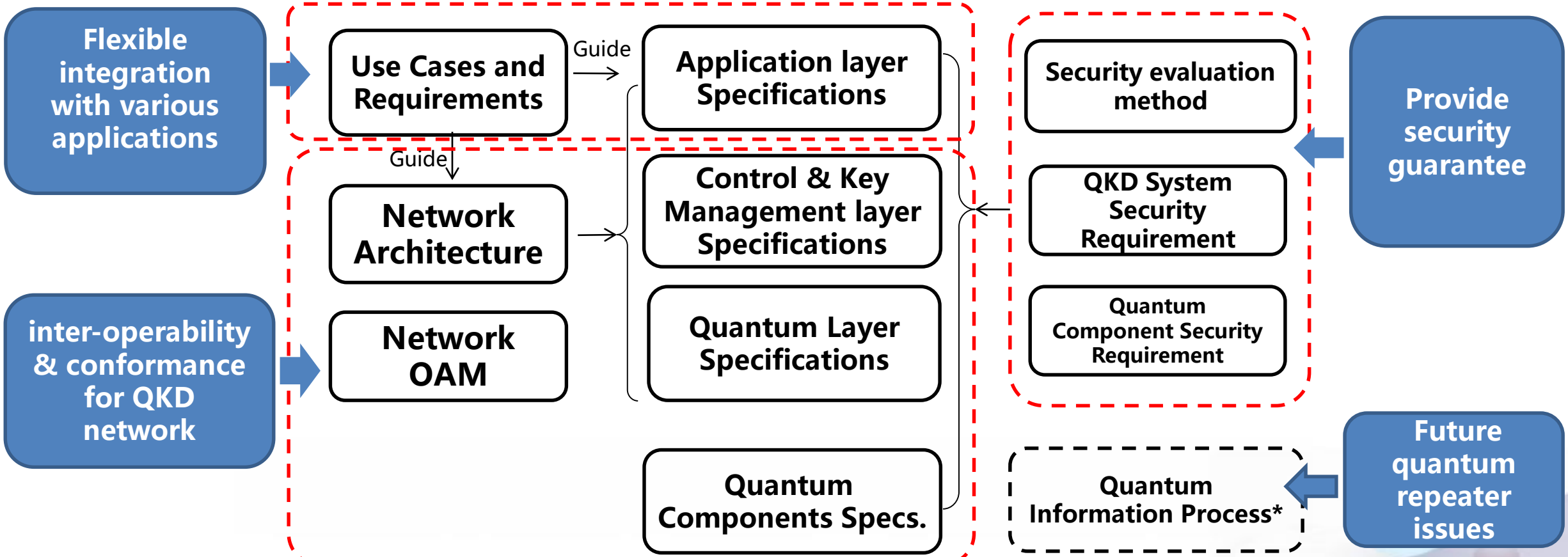
Network

- Design QKD network architecture and protocols:
  - To support scalability and inter-operability (domain/network/user)
  - To ensure conformance and reliability
  - To integrate with existing telecom infrastructure

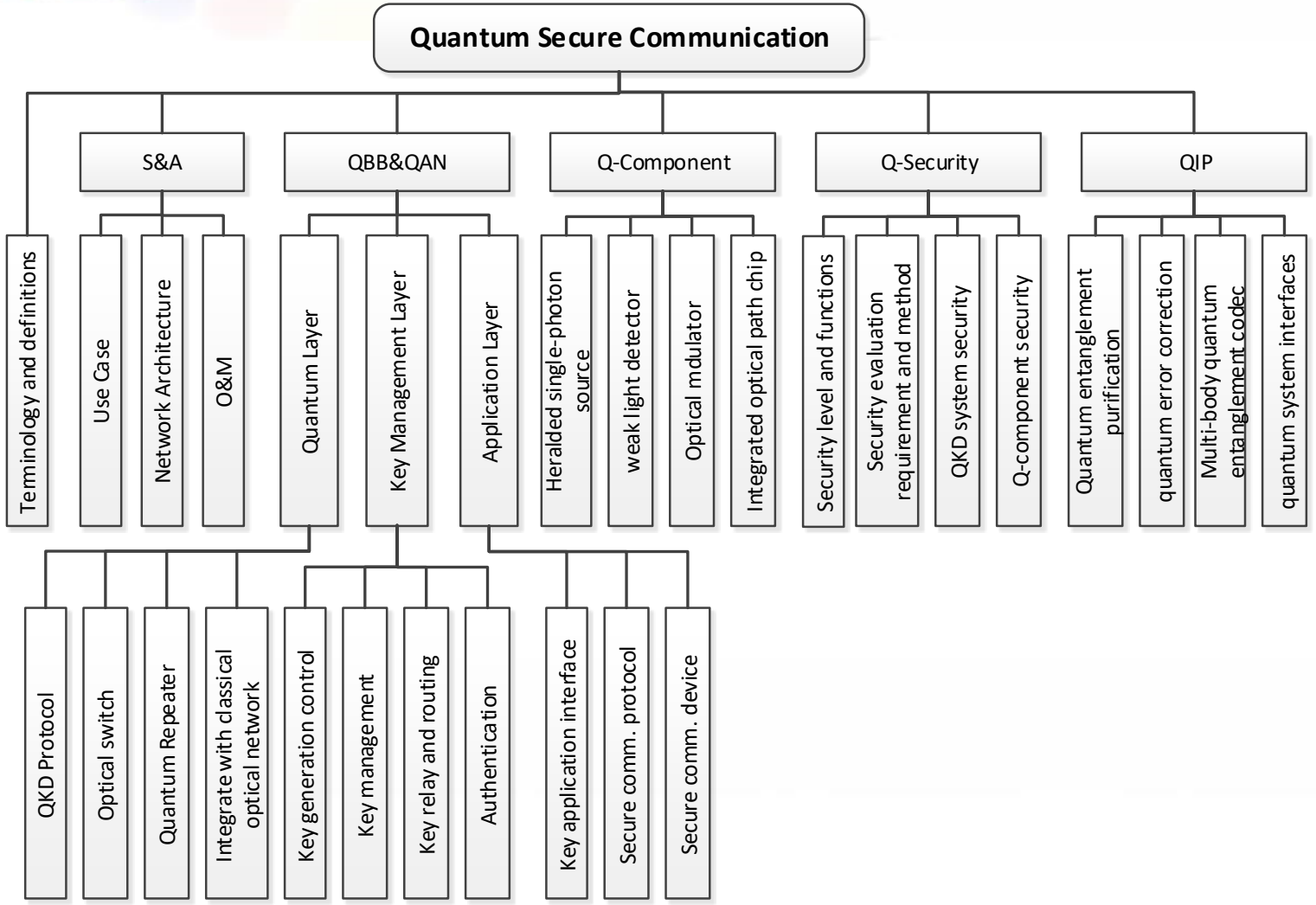
Security

- Provide security requirements and test methods for QKD implementations

Quantum-secured Communication Standardization Plan



Quantum-secured Communication standards framework



- **5 groups of standards:**
  - System and Architecture
  - Quantum Access & Backbone Network
  - Quantum Components
  - Quantum Security
  - Quantum information process

CCSA QSC standardization status

National Standards

1	Quantum Communication Terms and Definitions
2	Quantum Secure Communication application scenario and requirements

Industry Standards

1	Quantum Key Distribution (QKD) application interface
2	Technical requirements for quantum key distribution (QKD) systems Part I: Decoy-state BB84
3	Test methods of optical quantum key distribution (QKD) system
4	Quantum Secure Communication Network Architecture
5	Technical Requirements of Co-Fiber Transmission System for Quantum Key Distribution and Classic Optical Communication
6	Key components and modules for quantum key distribution (QKD) based on BB84 Protocol Part 1: optical source
7	Key components and modules for quantum key distribution (QKD) based on BB84 Protocol Part 2: Single photon detector
8	Key components and modules for quantum key distribution (QKD) based on BB84 Protocol Part 3: Quantum random number generator(QRNG)

Study Reports

1	Study on Quantum secure communication network architecture
2	Study on security issues of Quantum Key Distribution
3	Study on test and evaluation of Quantum Secure Communication System
4	Study on the Co-Fiber Transmission of Quantum Key Distribution and Classic Optical Communication Systems
5	Study on Generation and Test method of Quantum Random Number
6	Study on quantum key distribution key device and module Technology requirements
7	Study on Quantum Secure Communication Network Management
8	Study on CV-QKD technique
9	Study on software defined QKD network
10	Study on trusted relay node in QKD network
11	Study on Quantum Secure Communication Networking Key Technologies
12	Study on Freespace Quantum Secure Communication Technology
13	Requirements of encrypted data carried in MPLS PW in quantum secure communication network
14	Study on optimization protocol based on decoy state method

Progress:

- CCSA has initiated a series of work & study items according to the QSC standards framework
- 6 study reports have been finished: 6 study reports have been finished: QKD network architecture, QKD security issues, functional test method, co-fiber transmission, components and module requirements, quantum random number generation and test methods.

Contributions to international SDO:
—— Design considerations for QKD network

R1 Scalability

- Support MP-to-MP ITS Key transport
- Flexible and economic network expansion according to service growth
- Support flexible network topology for wide-area coverage
- Support one-to-many QKD for access network

R2 Efficiency

- Support efficient key supply and relay node routing schemes
- Provide high secret-key throughput and low latency to satisfy various application requirements

R3 Security

- Strict QKD protocol security proof and certification
- Effective countermeasures against known quantum layer threats
- Support effective security enhancements for trusted node

R4 Application-oriented

- Provide developer-friendly APIs for QKD network capabilities
- Facilitate integration with various ICT protocols and applications

R5 Robustness

- Fast fault detection and recovery when some nodes or links fail to ensure service continuity

R6 Interoperability

- Support multi-vendor interoperability for both QKD and network management devices

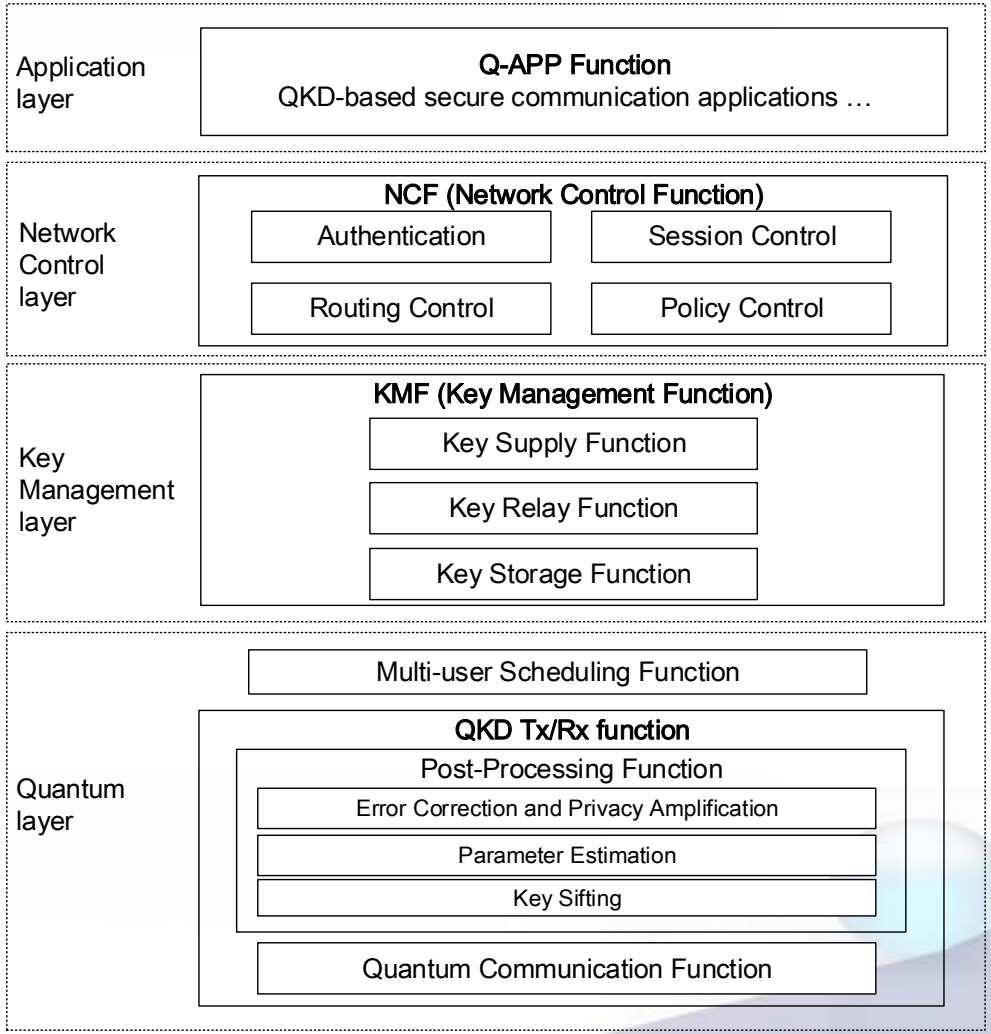
R7 Policy control

- Provide per-secret-key-flow QoS and Charging policy control and enforcement

* have been approved to be included in ITU-T Draft Recommendation Y.QKDN_FR

Contributions to international SDO: —— QKD network functional architecture

- to utilize the shared key pairs provided by the QKD network and perform encrypted communication between remote parties
- to control the QKD network resources to ensure efficiency, quality and capacity of QKD services
- to manage the keys generated by QKD links, transport the keys via the trusted nodes, and deliver the keys to the user applications
- to distribute keys to the authenticated transmitter and receiver of the QKD link using specific QKD protocol
- including multi-user scheduling capability

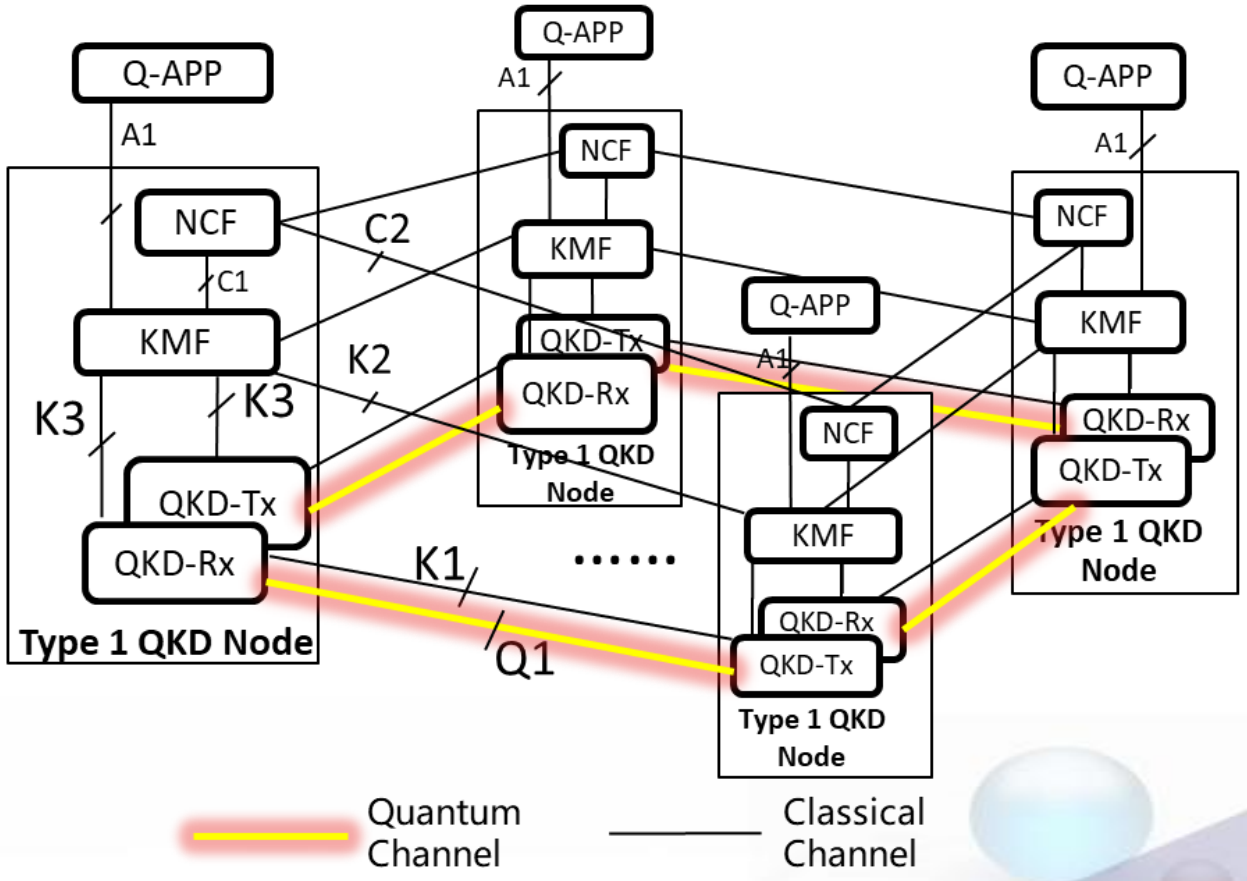


*** have been approved to be included in ITU-T Draft Recommendation Y.QKDN_Arch**

Contributions to international SDO: —— QKD network configurations

Configuration 1: Distributed mode

- In configuration 1, the QKD network is consisted of Type 1 QKD nodes.
- Each Type 1 QKD node can work in an self-organized manner independently.
- The Type 1 QKD node contains the functions of QKD-Tx/Rx, KMF and NCF.

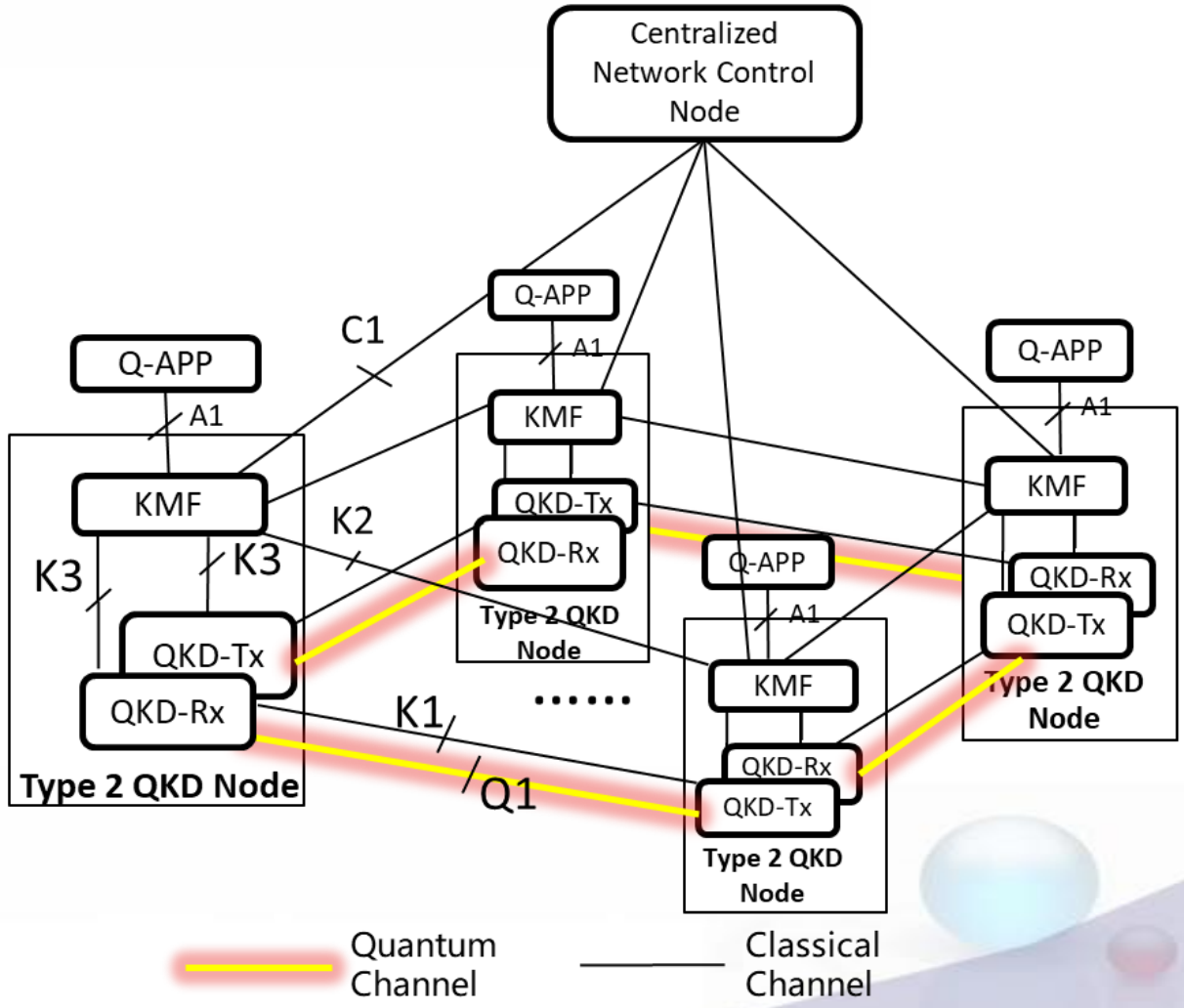


* have been approved to be included in ITU-T Draft Recommendation Y.QKDN_Arch

Contributions to international SDO: —— QKD network configurations

Configuration 2: Centralized network control mode

- to centralize the network control functions in order to reduce the complexity of QKD nodes and improve network control efficiency
- In configuration 2, the QKD network is consisted of Type 2 QKD nodes and the centralized network control nodes.
- The Type 2 QKD node contains the functions of QKD-Tx/Rx and KMF.

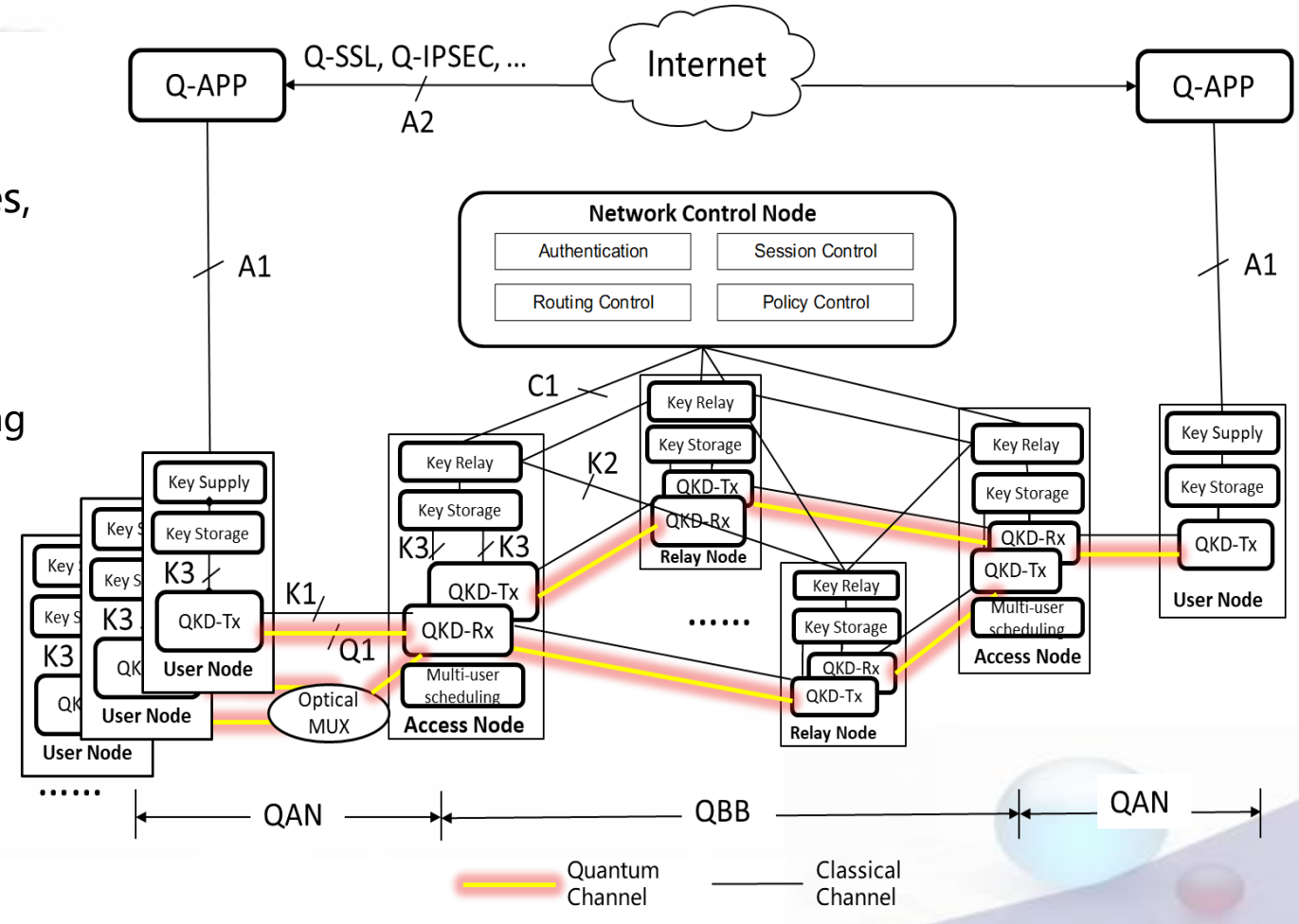


*** have been approved to be included in ITU-T Draft Recommendation Y.QKDN_Arch**

Contributions to international SDO: —— QKD network configurations

Configuration 3: Centralized network control with hierarchical QKD nodes

- To further reduce the complexity of QKD nodes, the Type 2 QKD node is further classified into QKDN user node, access node and relay node
- QKDN user node (Q-UN) : in charge of obtaining the key material from the QKD network, and providing the corresponding quantum key to a specific application for secure communication.
- QKDN access node (Q-AN): responsible for aggregating the associated Q-UNs' service flow and forwarding it to the remote QKD node
- QKDN relay node (Q-RN): to set up the IT-secure key relaying route in order to break the distance limitation of QKD quantum channels.

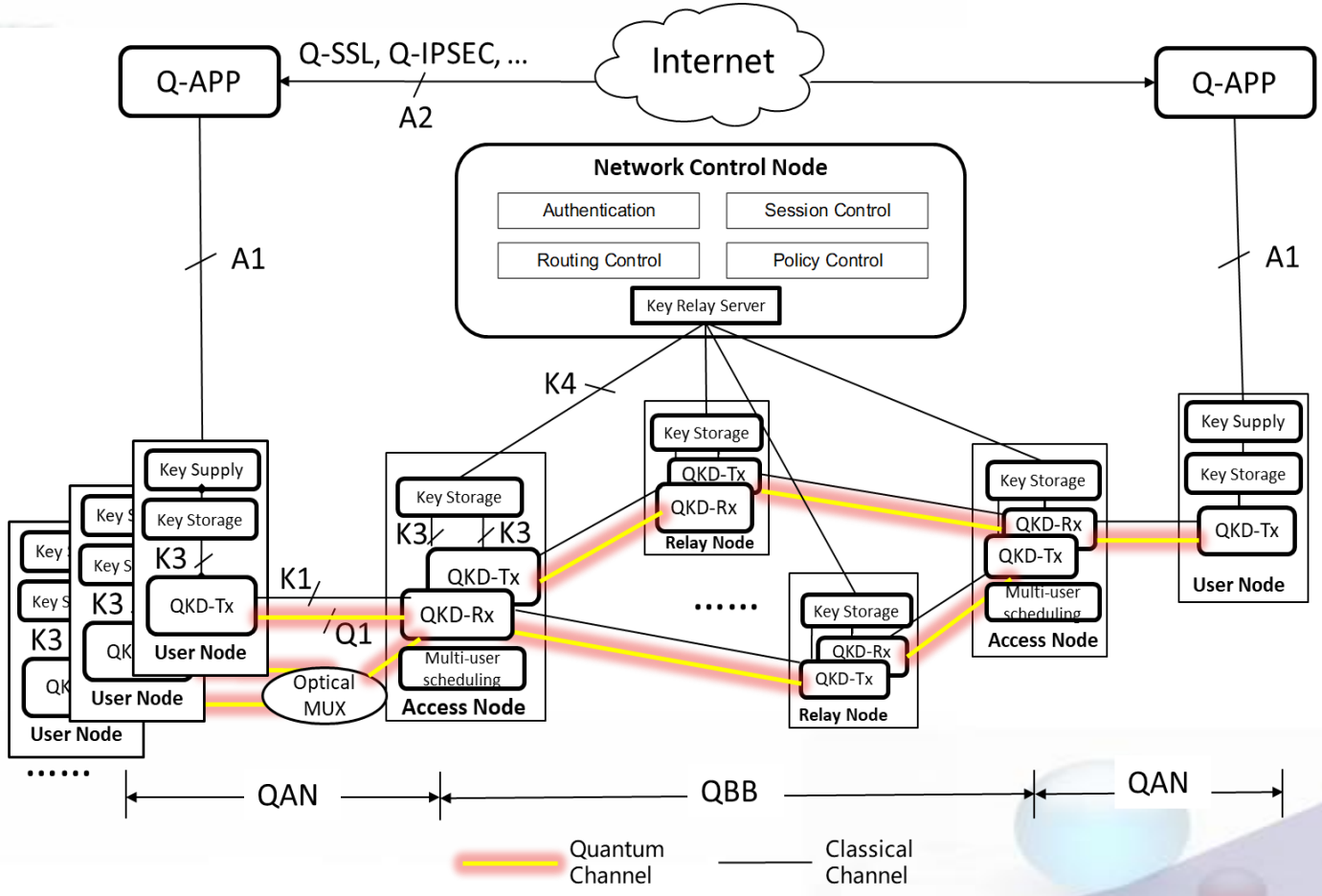


*** have been approved to be included in ITU-T Draft Recommendation Y.QKDN_Arch**

Contributions to international SDO: —— QKD network configurations

Configuration 4: Centralized network control and key relay mode

- In configuration 4, the key relaying function is centralized to further reduce the complexity of QKD nodes and enhance the security of QKD nodes.
- The function of key relay is removed from the Q-AN and Q-RN.
- And a centralized key relay server node is introduced which can be integrated within the network control node.



*** have been approved to be included in ITU-T Draft Recommendation Y.QKDN_Arch**

Suggestions for further QKD network standardization

Near term

- Standardize QKD network architecture and KM layer interfaces
- Standardize network level security requirements for trusted-relay-based QKD network

Ensure basic interoperability and security

Long term

- Co-fiber transmission of quantum and classical signals
- Explore new use cases, e.g., integration of QKD and classical cryptography (including PQC)
- Study quantum network connected via quantum repeaters

……

Lower down cost

Bring more value

Achieve quantum comm. scalability

Summary

- Developing QKD standards including link level, system level, security evaluation and certification is urgent to support QKD network deployment and application.
- The success of QKD industry requires multi-disciplinary collaboration: quantum physics, communication networks, cryptography, information security, etc.
- There is strong need to coordinate and strengthen cooperation with different SDOs to push forward related work in an efficient manner.

Thanks!
Q&A