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
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

Flexible integration with various applications

inter-operability & conformance for QKD network

Use Cases and Requirements

Network Architecture

Network OAM

Application layer Specifications

Control & Key Management layer Specifications

Quantum Layer Specifications

Quantum Component Specifications

Security evaluation method

QKD System Security Requirement

Quantum Component Security Requirement

Quantum Information Process*

Provide security guarantee

Future quantum repeater issues

Flexible integration with various applications

inter-operability & conformance for QKD network

Use Cases and Requirements

Network Architecture

Network OAM

Application layer Specifications

Control & Key Management layer Specifications

Quantum Layer Specifications

Quantum Component Specifications

Security evaluation method

QKD System Security Requirement

Quantum Component Security Requirement

Quantum Information Process*

Provide security guarantee

Future quantum repeater issues

Flexible integration with various applications

inter-operability & conformance for QKD network

Use Cases and Requirements

Network Architecture

Network OAM

Application layer Specifications

Control & Key Management layer Specifications

Quantum Layer Specifications

Quantum Component Specifications

Security evaluation method

QKD System Security Requirement

Quantum Component Security Requirement

Quantum Information Process*

Provide security guarantee

Future quantum repeater issues
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

Progress:
- CCSA has initiated a series of work & study items according to the QSC standards framework.
- 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

<table>
<thead>
<tr>
<th>Requirement</th>
<th>R1 Scalability</th>
<th>R2 Efficiency</th>
<th>R3 Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support MP-to-MP ITS Key transport</td>
<td>• Support MP-to-MP ITS Key transport</td>
<td>• Support efficient key supply and relay node routing schemes</td>
<td>• Strict QKD protocol security proof and certification</td>
</tr>
<tr>
<td>Flexible and economic network expansion according to service growth</td>
<td>• Flexible and economic network expansion according to service growth</td>
<td>• Provide high secret-key throughput and low latency to satisfy various application requirements</td>
<td>• Effective countermeasures against known quantum layer threats</td>
</tr>
<tr>
<td>Support flexible network topology for wide-area coverage</td>
<td>• Support flexible network topology for wide-area coverage</td>
<td>• Support one-to-many QKD for access network</td>
<td>• Support effective security enhancements for trusted node</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Requirement</th>
<th>R4 Application-oriented</th>
<th>R5 Robustness</th>
<th>R6 Interoperability</th>
<th>R7 Policy control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provide developer-friendly APIs for QKD network capabilities</td>
<td>• Provide developer-friendly APIs for QKD network capabilities</td>
<td>• Fast fault detection and recovery when some nodes or links fail to ensure service continuity</td>
<td>• Support multi-vendor interoperability for both QKD and network management devices</td>
<td>• Provide per-secret-key-flow QoS and Charging policy control and enforcement</td>
</tr>
<tr>
<td>Facilitate integration with various ICT protocols and applications</td>
<td>• Facilitate integration with various ICT protocols and applications</td>
<td>• Fast fault detection and recovery when some nodes or links fail to ensure service continuity</td>
<td>• Support multi-vendor interoperability for both QKD and network management devices</td>
<td>• Provide per-secret-key-flow QoS and Charging policy control and enforcement</td>
</tr>
</tbody>
</table>

* have been approved to be included in ITU-T Draft Recommendation Y.QKDN_FR
## Contributions to international SDO: QKD network functional architecture

<table>
<thead>
<tr>
<th>Layer</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Application layer</strong></td>
<td>Q-APP Function</td>
</tr>
<tr>
<td><strong>Network Control layer</strong></td>
<td>NCF (Network Control Function)</td>
</tr>
<tr>
<td></td>
<td>Authentication</td>
</tr>
<tr>
<td></td>
<td>Routing Control</td>
</tr>
<tr>
<td><strong>Key Management layer</strong></td>
<td>KMF (Key Management Function)</td>
</tr>
<tr>
<td></td>
<td>Key Supply Function</td>
</tr>
<tr>
<td></td>
<td>Key Relay Function</td>
</tr>
<tr>
<td></td>
<td>Key Storage Function</td>
</tr>
<tr>
<td><strong>Quantum layer</strong></td>
<td>QKD Tx/Rx function</td>
</tr>
<tr>
<td></td>
<td>Post-Processing Function</td>
</tr>
<tr>
<td></td>
<td>Error Correction and Privacy Amplification</td>
</tr>
<tr>
<td></td>
<td>Parameter Estimation</td>
</tr>
<tr>
<td></td>
<td>Key Sifting</td>
</tr>
<tr>
<td></td>
<td>Quantum Communication Function</td>
</tr>
</tbody>
</table>

- 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
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
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
**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

• 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

……

Long term

Ensure basic interoperability and security

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